Chapter 4: Wireless LANs

Scaling Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 4

4.0 Introduction

4.1 Wireless LAN Concepts

4.2 Wireless LAN Operations

4.3 Wireless LAN Security

4.4 Wireless LAN Configuration

4.5 Summary

Chapter 4: Objectives

- Describe wireless LAN technology and standards.
- Describe the components of a wireless LAN infrastructure.
- Describe wireless topologies.
- Describe the 802.11 frame structure.
- Describe the media contention method used by wireless technology.
- Describe channel management in a WLAN.
- Describe threats to wireless LANs.
- Describe wireless LAN security mechanisms.
- Configure a wireless router to support a remote site.
- Configure wireless clients to connect to a wireless router.
- Troubleshoot common wireless configuration issues.

4.1 Wireless Concepts

Cisco Networking Academy®
Mind Wide Open™

WLAN Components

Supporting Mobility

- Productivity is no longer restricted to a fixed work location or a defined time period.
- People now expect to be connected at any time and place, from the office to the airport or the home.
- Users now expect to be able to roam wirelessly.
- Roaming enables a wireless device to maintain Internet access without losing a connection.

WLAN Components

Benefits of Wireless

- Increased flexibility
- Increased productivity
- Reduced costs
- Ability to grow and adapt to changing requirements

WLAN Components

Wireless Technologies

Wireless networks can be classified broadly as:

- **Wireless personal-area network (WPAN)** – Operates in the range of a few feet (Bluetooth).
- **Wireless LAN (WLAN)** – Operates in the range of a few hundred feet.
- **Wireless wide-area network (WWAN)** – Operates in the range of miles.
- **Bluetooth** – An IEEE 802.15 WPAN standard; uses a device-pairing process to communicate over distances up to .05 mile (100m).
- **Wi-Fi (wireless fidelity)** – An IEEE 802.11 WLAN standard; provides network access to home and corporate users, to include data, voice and video traffic, to distances up to 0.18 mile (300m).

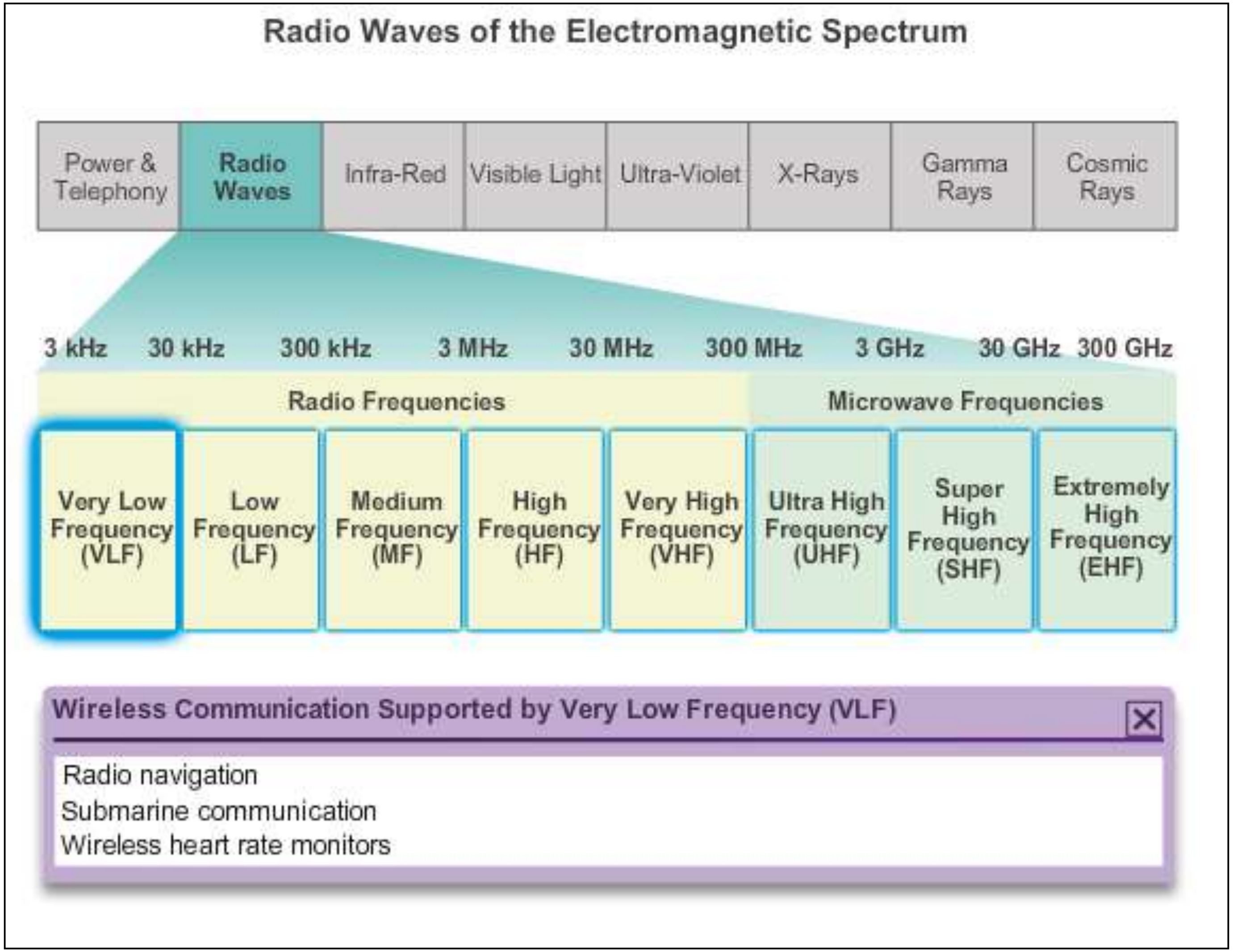
WLAN Components

Wireless Technologies (cont.)

- **Worldwide Interoperability for Microwave Access (WiMAX)** – An IEEE 802.16 WWAN standard that provides wireless broadband access of up to 30 mi (50 km).
- **Cellular broadband** – Consists of various corporate, national, and international organizations using service provider cellular access to provide mobile broadband network connectivity.
- **Satellite Broadband** – Provides network access to remote sites through the use of a directional satellite dish.

WLAN Components

Radio Frequencies



Radio Waves of the Electromagnetic Spectrum

Power & Telephony | Radio Waves | Infra-Red | Visible Light | Ultra-Violet | X-Rays | Gamma Rays | Cosmic Rays

3 kHz 30 kHz 300 kHz 3 MHz 30 MHz 300 MHz 3 GHz 30 GHz 300 GHz

Radio Frequencies

Microwave Frequencies

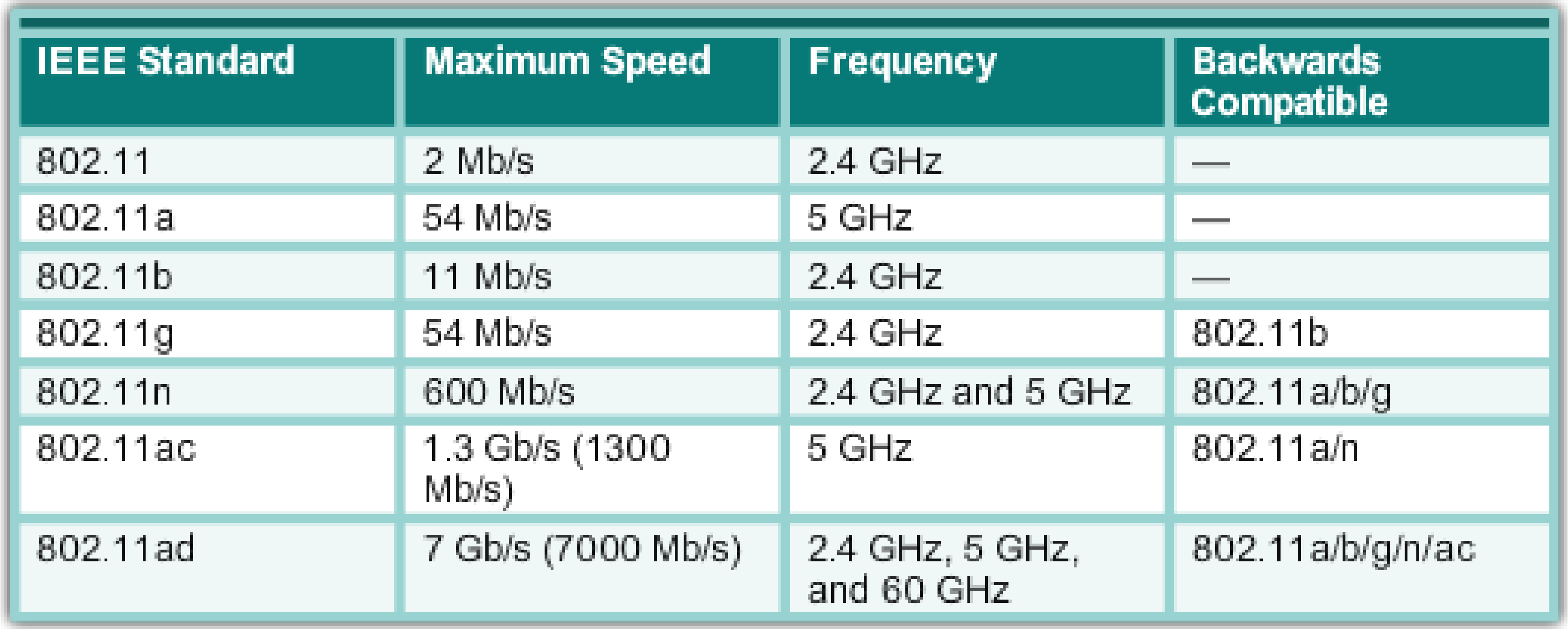
Very Low Frequency (VLF) | Low Frequency (LF) | Medium Frequency (MF) | High Frequency (HF) | Very High Frequency (VHF) | Ultra High Frequency (UHF) | Super High Frequency (SHF) | Extremely High Frequency (EHF)

Wireless Communication Supported by Very Low Frequency (VLF) ☒

Radio navigation
Submarine communication
Wireless heart rate monitors

WLAN Components

802.11 Standards



IEEE Standard	Maximum Speed	Frequency	Backwards Compatible
802.11	2 Mb/s	2.4 GHz	—
802.11a	54 Mb/s	5 GHz	—
802.11b	11 Mb/s	2.4 GHz	—
802.11g	54 Mb/s	2.4 GHz	802.11b
802.11n	600 Mb/s	2.4 GHz and 5 GHz	802.11a/b/g
802.11ac	1.3 Gb/s (1300 Mb/s)	5 GHz	802.11a/n
802.11ad	7 Gb/s (7000 Mb/s)	2.4 GHz, 5 GHz, and 60 GHz	802.11a/b/g/n/ac

WLAN Components

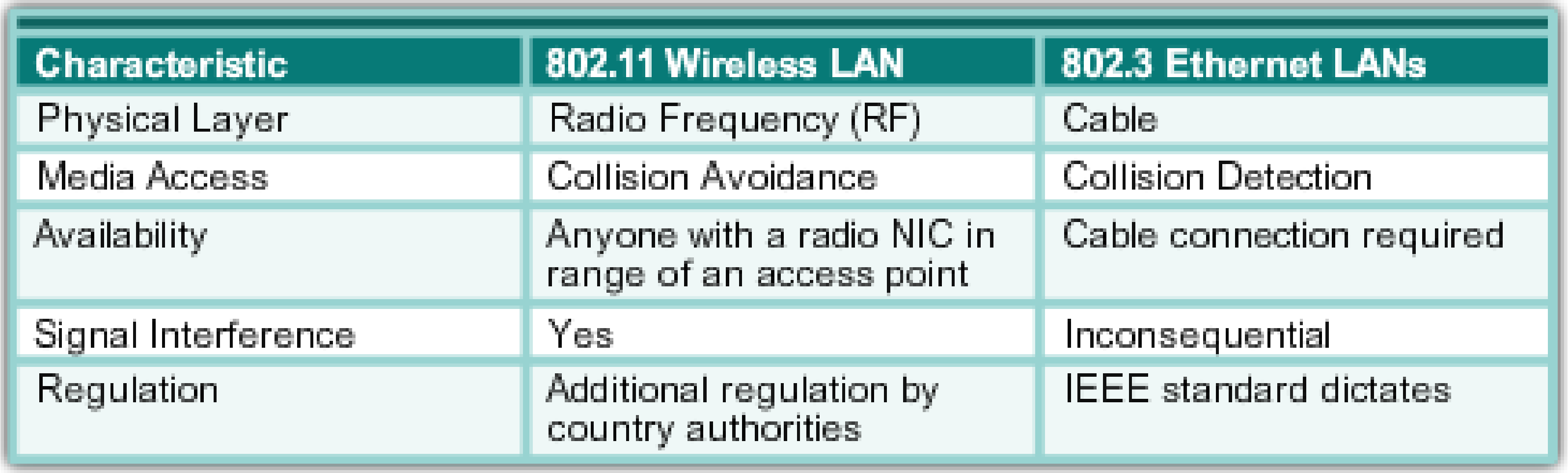
Wi-Fi Certification

The Wi-Fi Alliance certifies Wi-Fi and the following product compatibility:

- IEEE 802.11a/b/g/n/ac/ad-compatible.
- IEEE 802.11i secure using WPA2™ and Extensible Authentication Protocol (EAP)
- Wi-Fi Protected Setup (WPS) to simplify device connections.
- Wi-Fi Direct to share media between devices
- Wi-Fi Passpoint to simplify securely connecting to Wi-Fi hotspot networks
- Wi-Fi Miracast to seamlessly display video between devices

WLAN Components

Comparing WLANs to LANs



Characteristic	802.11 Wireless LAN	802.3 Ethernet LANs
Physical Layer	Radio Frequency (RF)	Cable
Media Access	Collision Avoidance	Collision Detection
Availability	Anyone with a radio NIC in range of an access point	Cable connection required
Signal Interference	Yes	Inconsequential
Regulation	Additional regulation by country authorities	IEEE standard dictates

Components of WLANs

Wireless NICs

Wireless deployment requires:

- End devices with wireless NICs
- Infrastructure device, such as a wireless router or wireless AP

Wireless USB Adapters

Linksys AE6000 Mini USB Wi-Fi Wireless-AC Dual-Band Adapter 2.4 or 5 GHz 802.11ac

Linksys AE3000 High Performance Dual-Band N USB Adapter

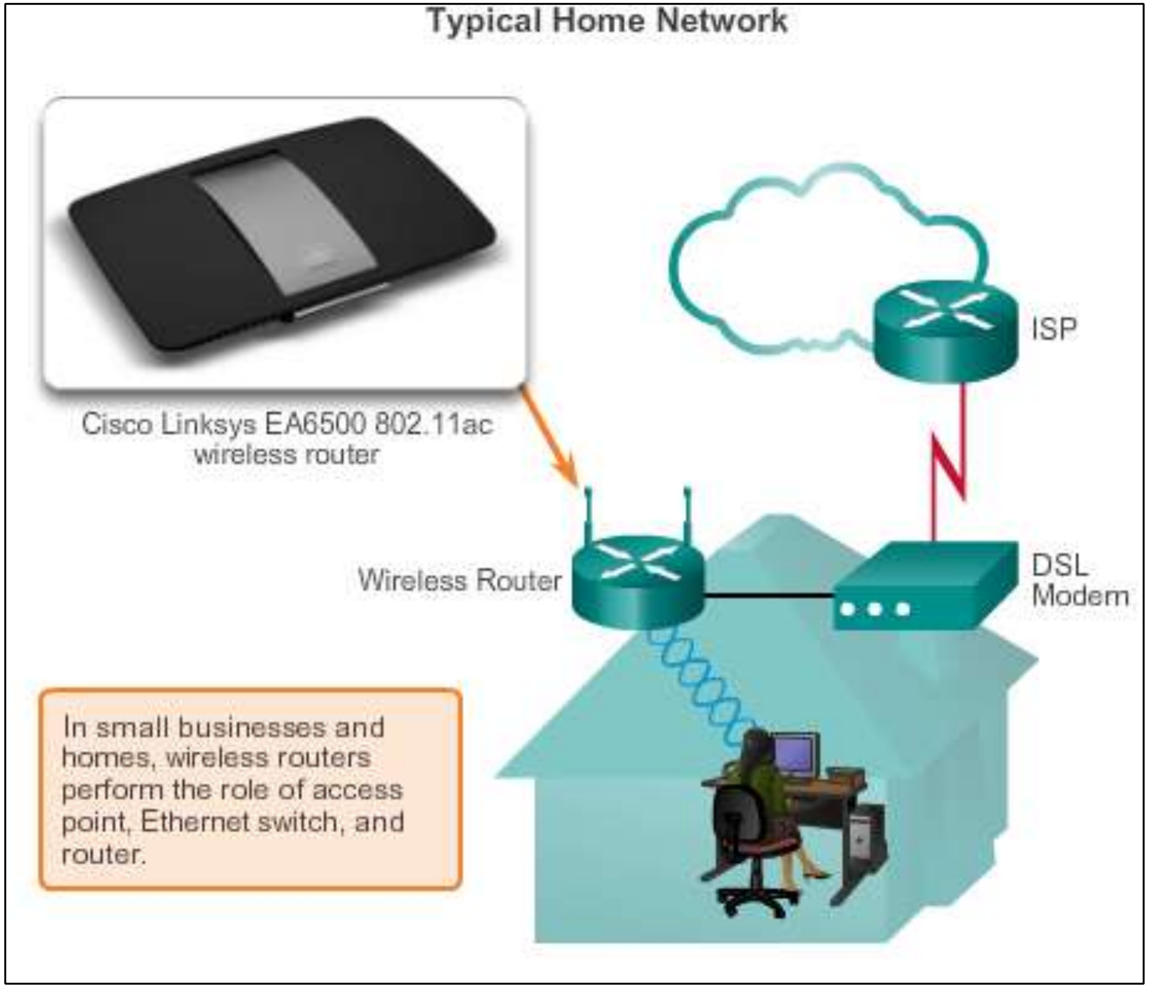
Components of WLANs

Wireless Home Router

A home user typically interconnects wireless devices using a small, integrated wireless router.

These serve as:

- access point
- Ethernet switch
- router

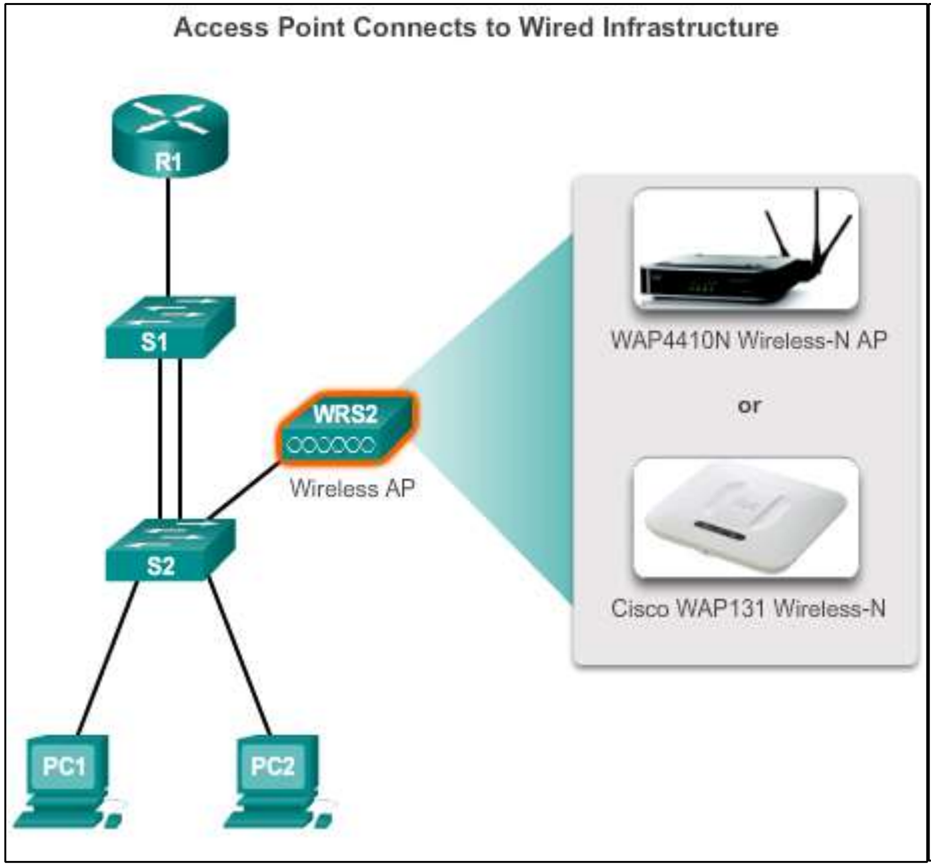


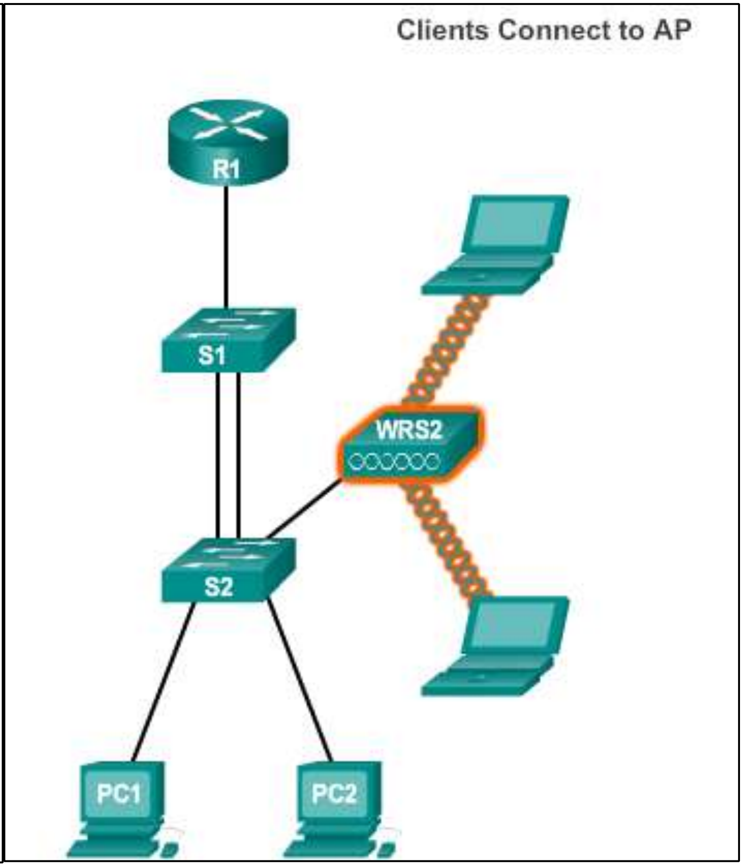
Typical Home Network

In small businesses and homes, wireless routers perform the role of access point, Ethernet switch, and router.

Components of WLANs

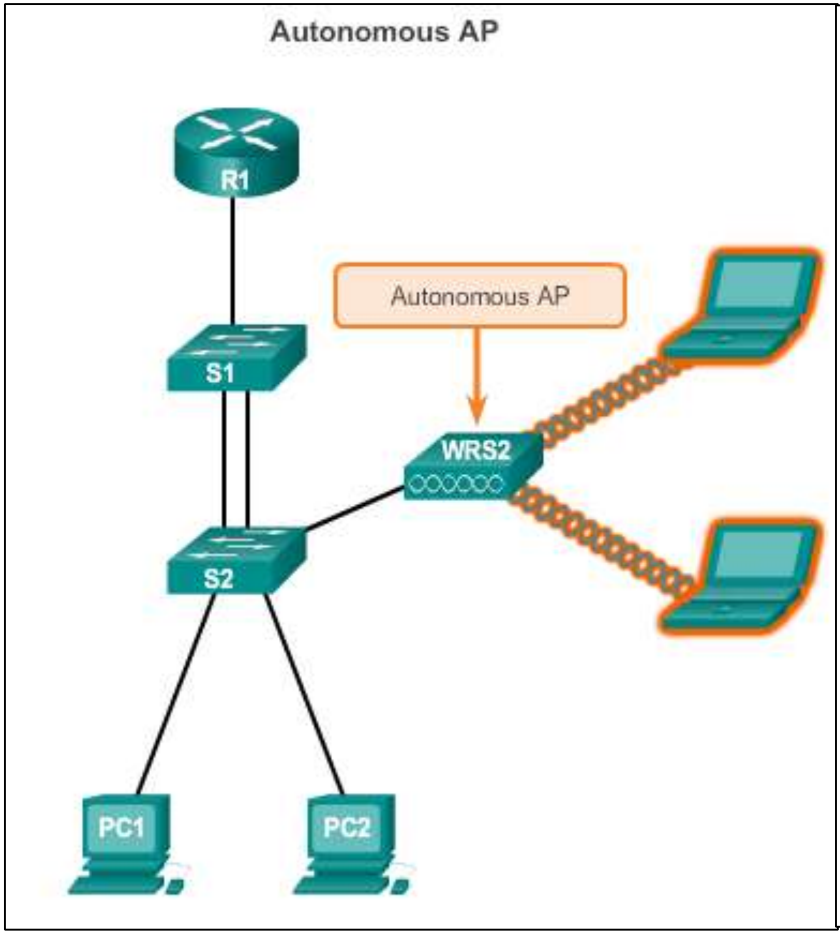
Business Wireless Solutions


Access Point Connects to Wired Infrastructure

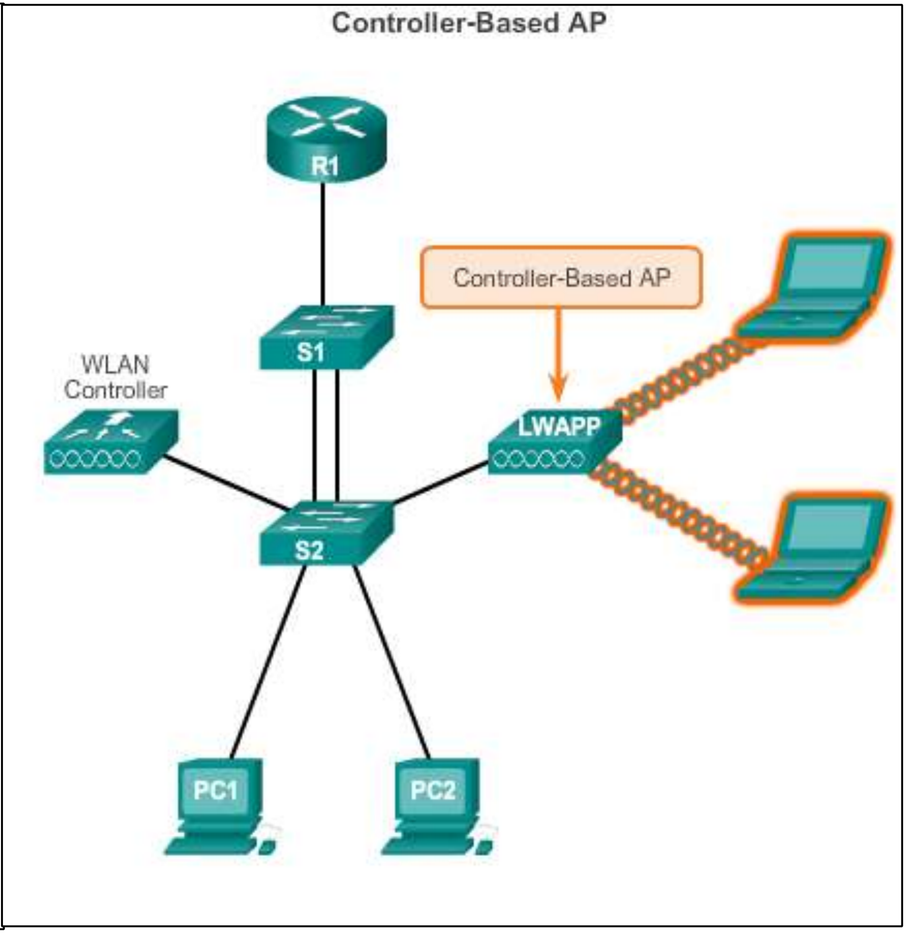

Clients Connect to AP

Components of WLANs

Wireless Access Points



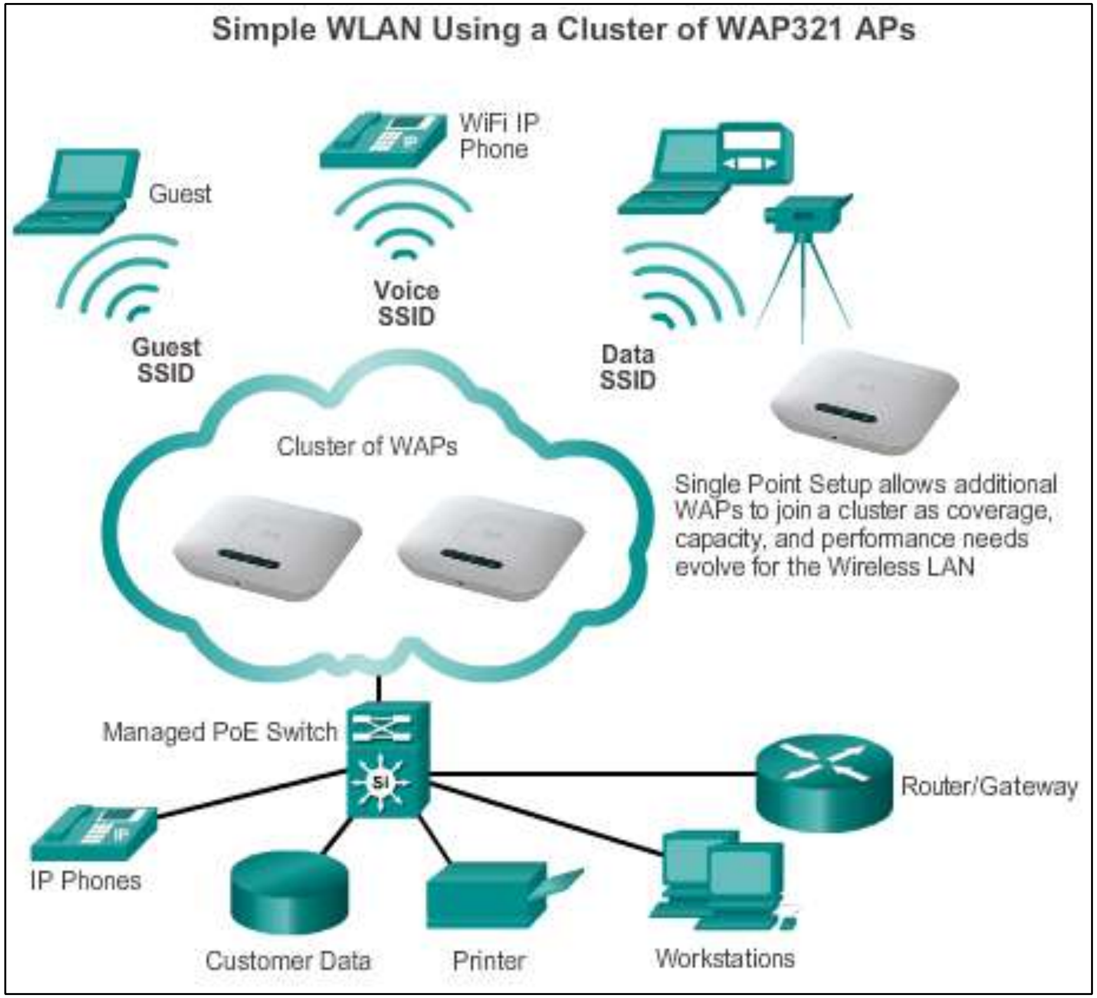
Autonomous AP



Controller-Based AP

Components of WLANs

Small Wireless Deployment Solutions



Single Point Setup allows additional WAPs to join a cluster as coverage, capacity, and performance needs evolve for the Wireless LAN

- Support the clustering of APs without the use of a controller.
- Multiple APs can be deployed and pushed to a single configuration to all devices within the cluster, managing the wireless network as a single system without worrying about interference between APs, and without configuring each AP as a separate device.

Components of WLANs

Large Wireless Deployment Solutions (cont.)

Controller-Based Wireless APs

Cisco Aironet 1600, 2600, and 3600 Series
Robust controller-based APs

Cisco Aironet 600 Series OfficeExtend
Used to extend 802.11n wireless coverage to the home teleworking environment

Cisco 1552 Series Outdoor Rugged APs
Robust outdoor controller-based AP

Components of WLANs

Large Wireless Deployment Solutions (cont.)

Controllers for Small and Medium-Sized Businesses

Cisco Virtual Controller

Cisco Wireless Controller on the Cisco Services Ready Engine (SRE)

Cisco Wireless Controller on the Cisco Services Ready Engine (SRE)

Components of WLANs
Wireless Antennas

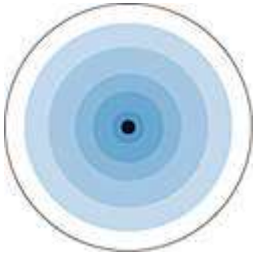
Cisco Aironet APs can use:

- **Omnidirectional Wi-Fi Antennas** – Factory Wi-Fi gear often uses basic dipole antennas, also referred to as “rubber duck” design, similar to those used on walkie-talkie radios. Omnidirectional antennas provide 360-degree coverage.
- **Directional Wi-Fi Antennas** – Directional antennas focus the radio signal in a given direction, which enhances the signal to and from the AP in the direction the antenna is pointing.
- **Yagi antennas** – Type of directional radio antenna that can be used for long-distance Wi-Fi networking.

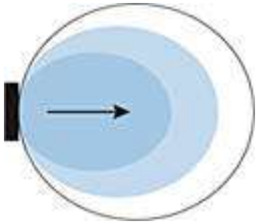
Components of WLANs

Wireless Antennas

Omnidirectional



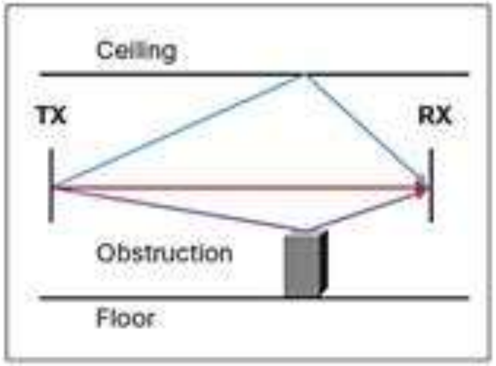
Directional

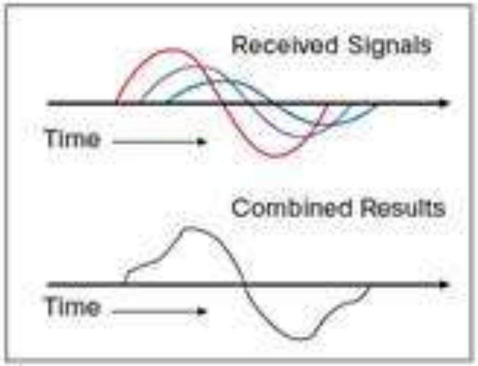


Components of WLANs

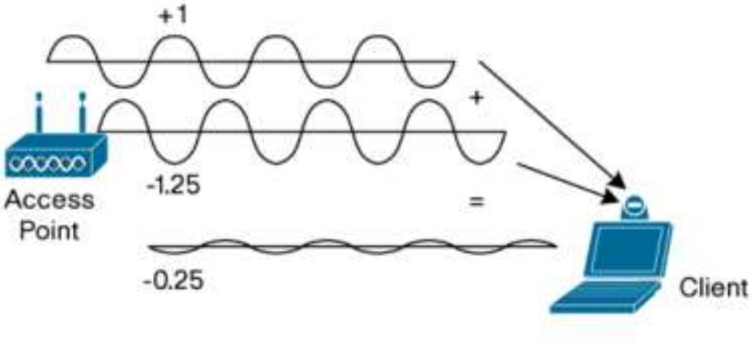
Wireless Antennas

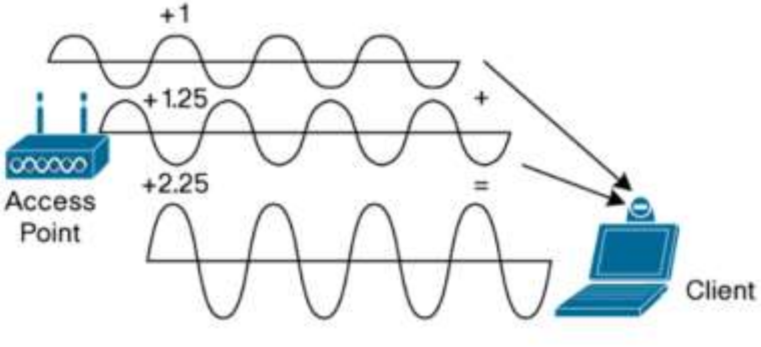
Multipath Distortion





Transmit Beamforming

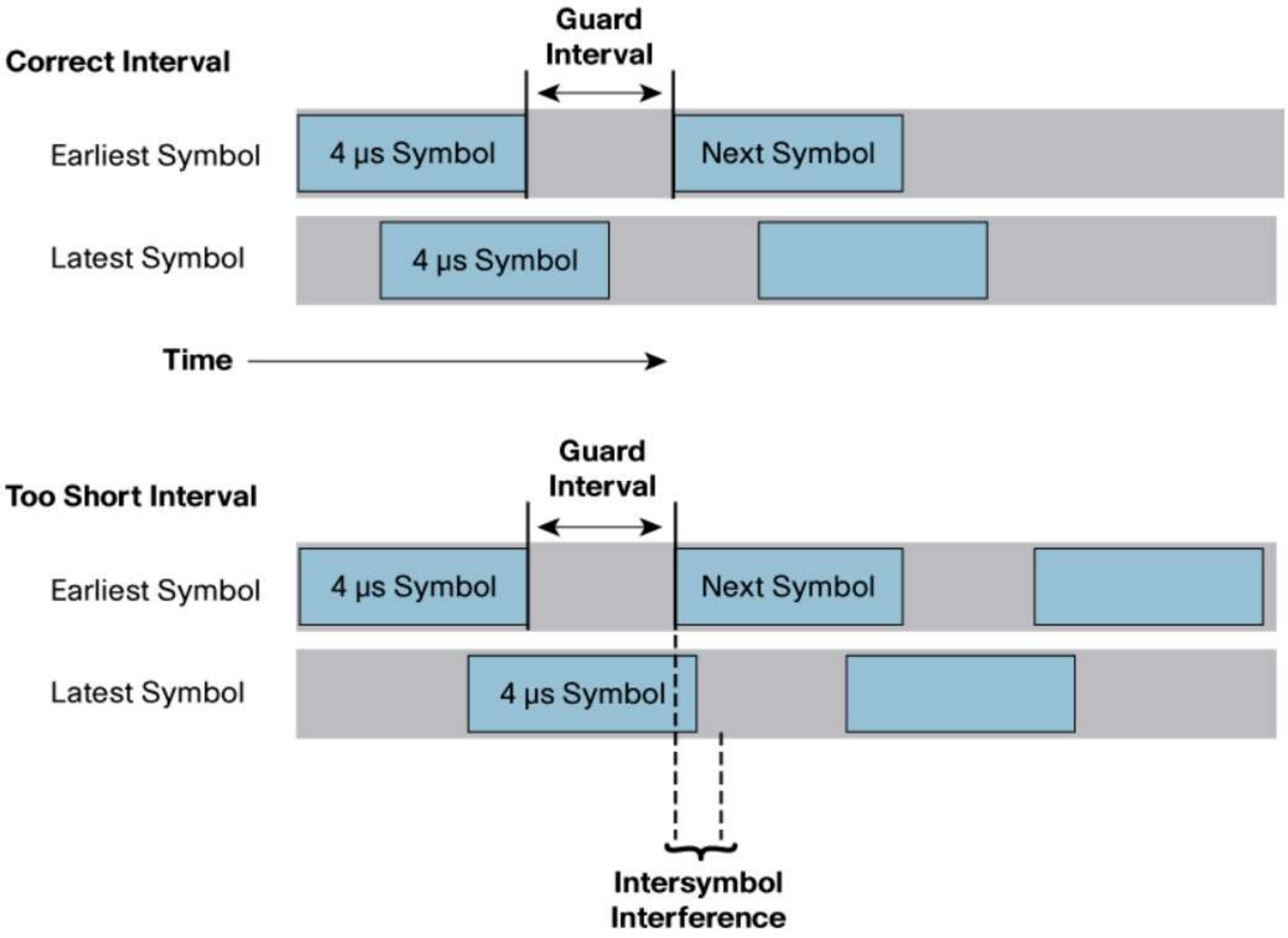




Components of WLANs

Wireless Antennas

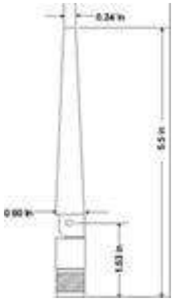
Inter symbol guard interval

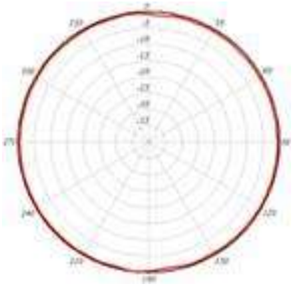


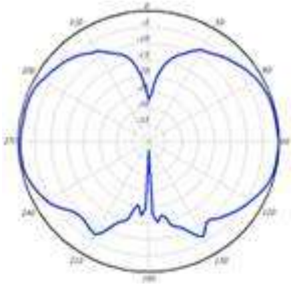
Components of WLANs

Wireless Antennas

Rubber duck antenna



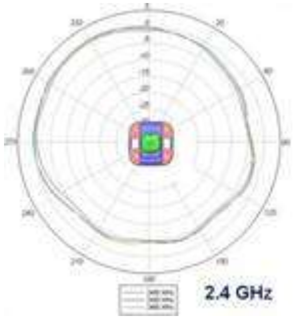


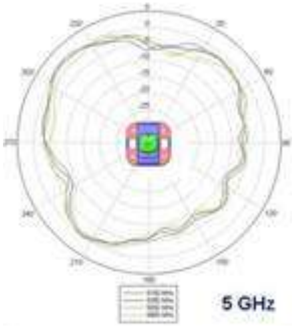


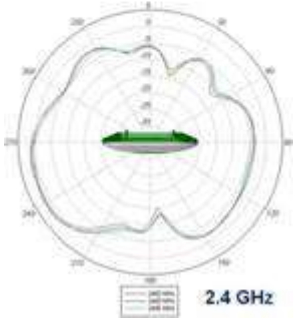
Components of WLANs

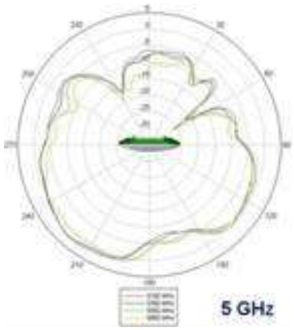
Wireless Antennas

Aironet 3600i Series Integrated Antennas



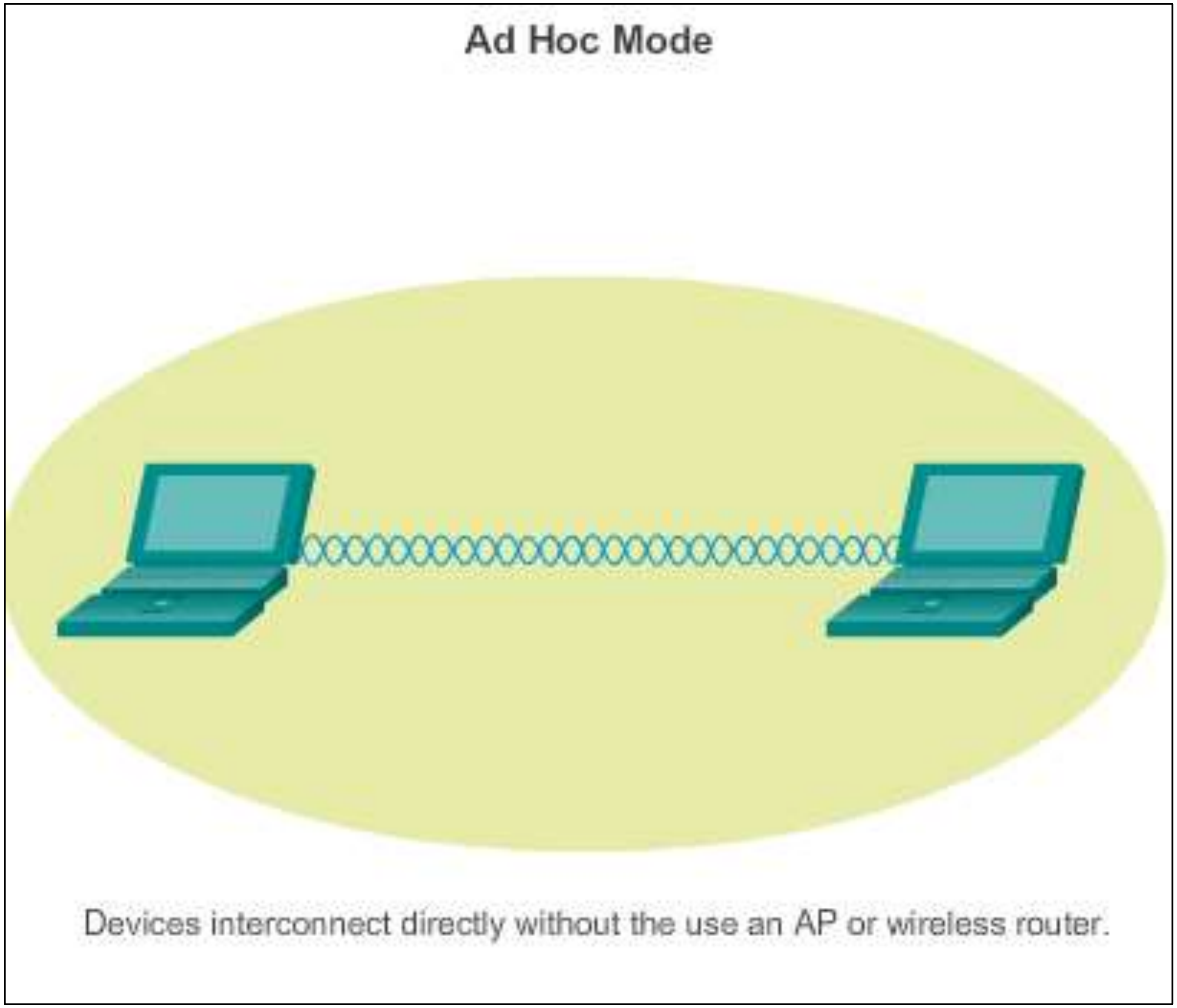






802.11 WLAN Topologies

802.11 Wireless Topology Modes

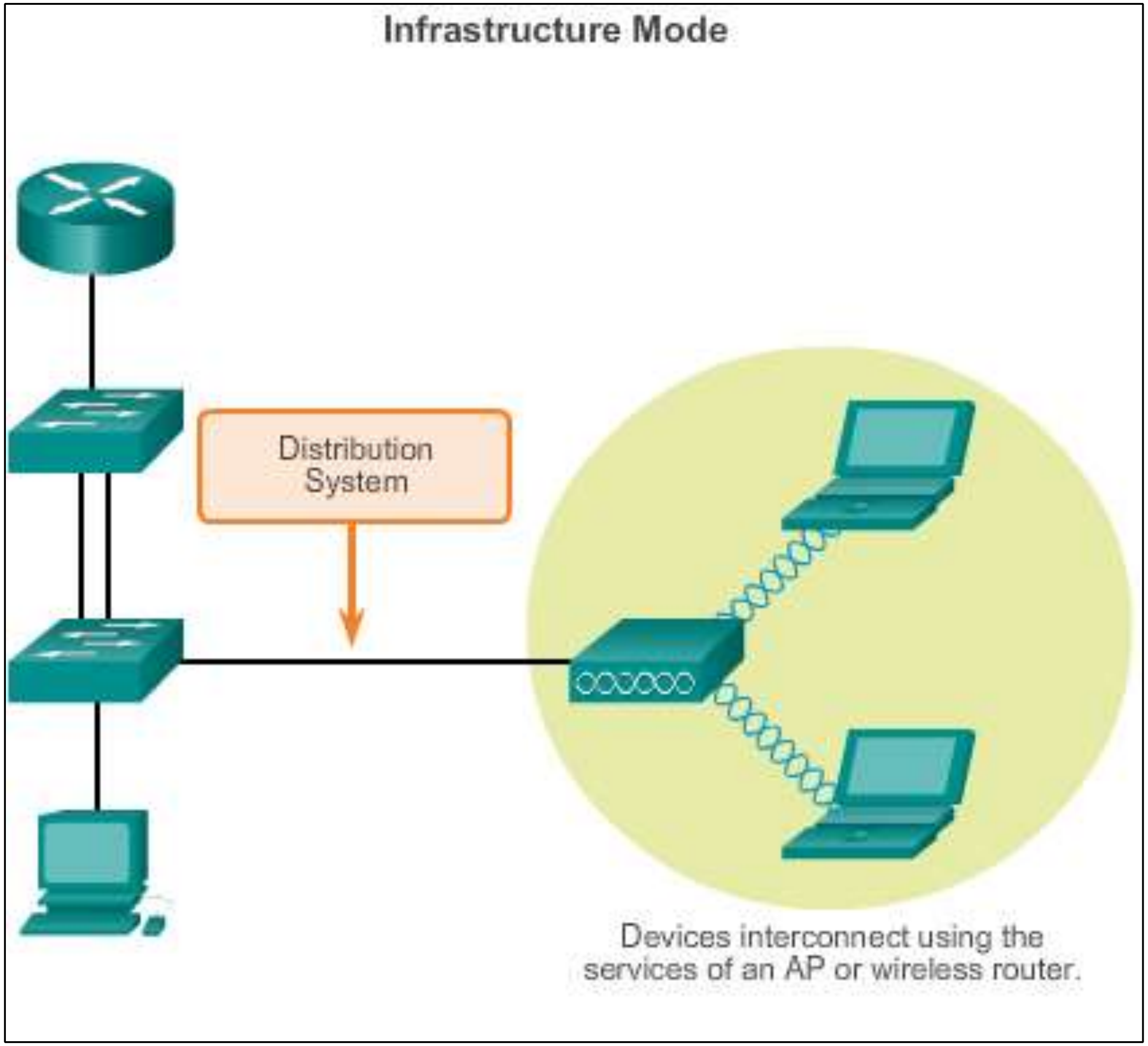


Ad Hoc Mode

Devices interconnect directly without the use an AP or wireless router.

802.11 WLAN Topologies

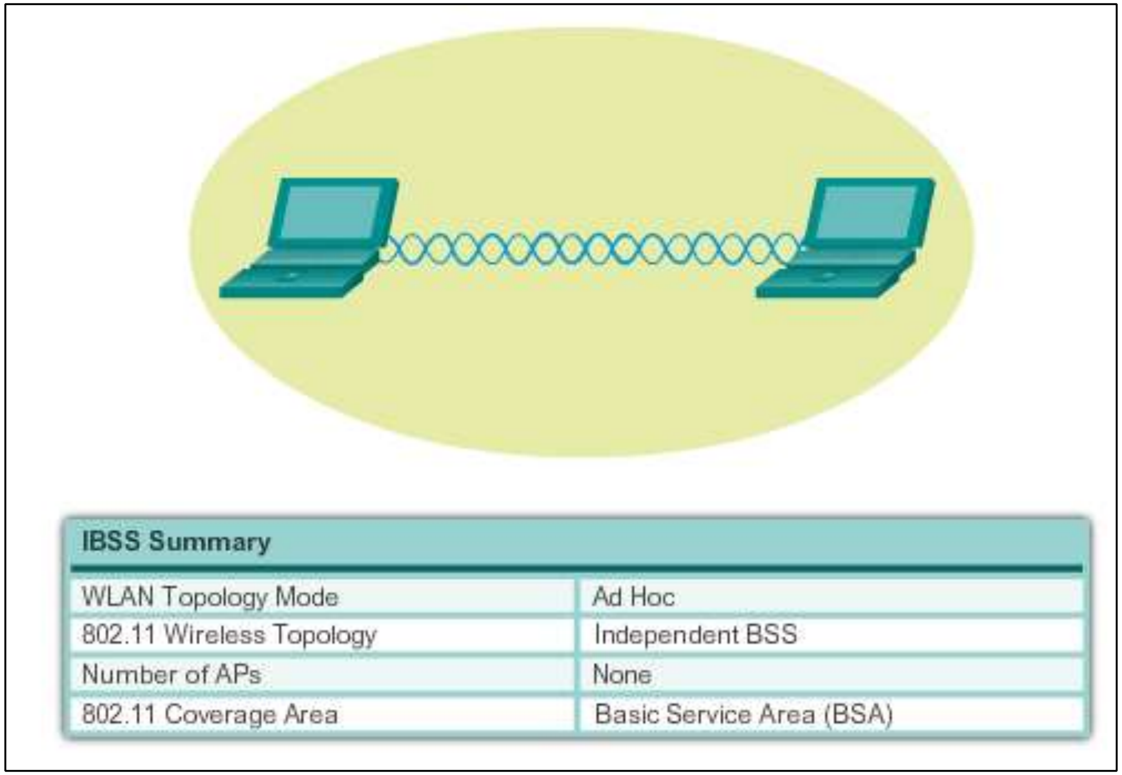
802.11 Wireless Topology Modes (cont.)


Infrastructure Mode
Distribution System
Devices interconnect using the services of an AP or wireless router.

802.11 WLAN Topologies

Ad Hoc Mode

Tethering (personal hotspot) – Variation of the Ad Hoc topology when a smart phone or tablet with cellular data access is enabled to create a personal hotspot.

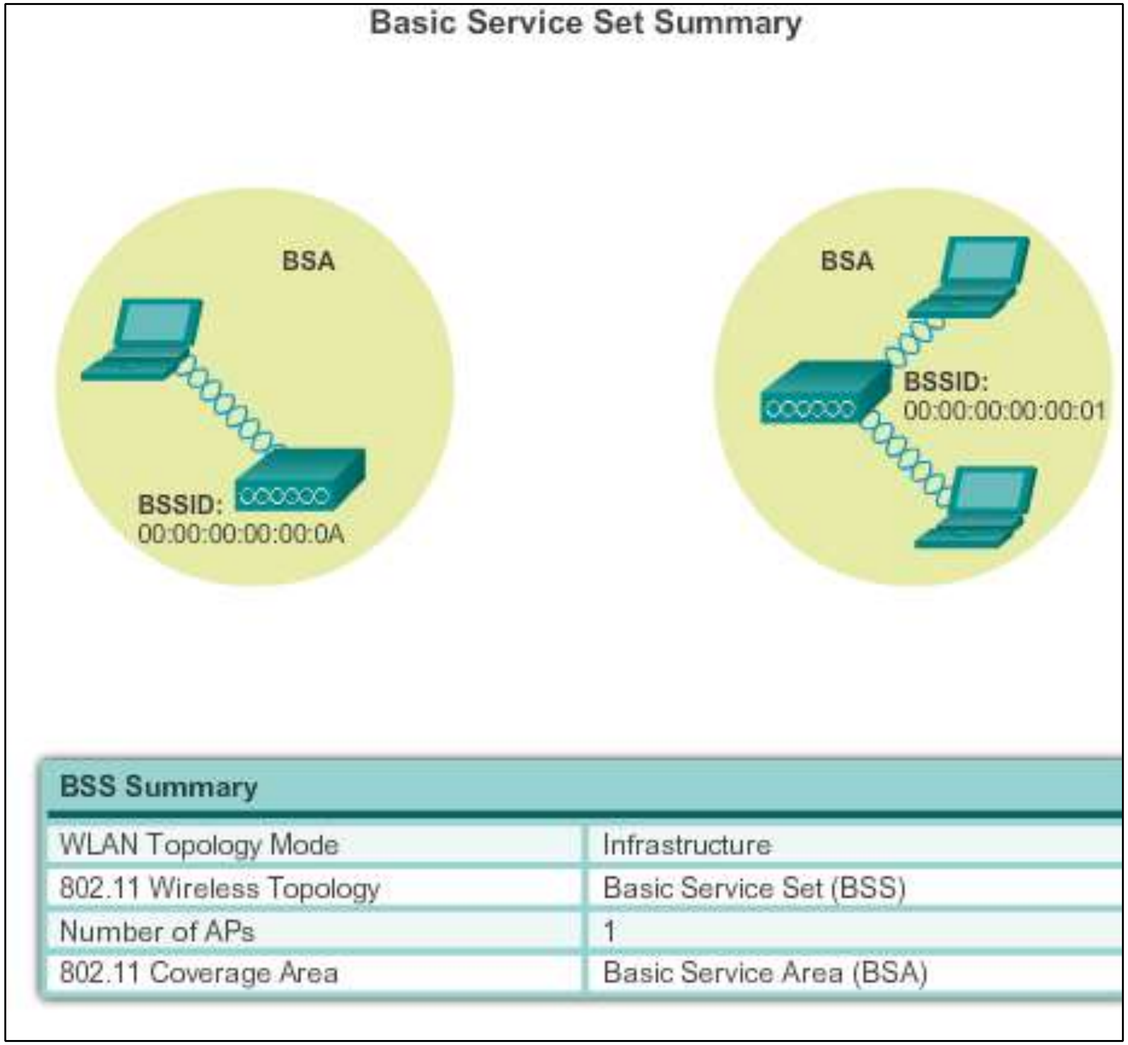


IBSS Summary

WLAN Topology Mode	Ad Hoc
802.11 Wireless Topology	Independent BSS
Number of APs	None
802.11 Coverage Area	Basic Service Area (BSA)

802.11 WLAN Topologies

Infrastructure Mode

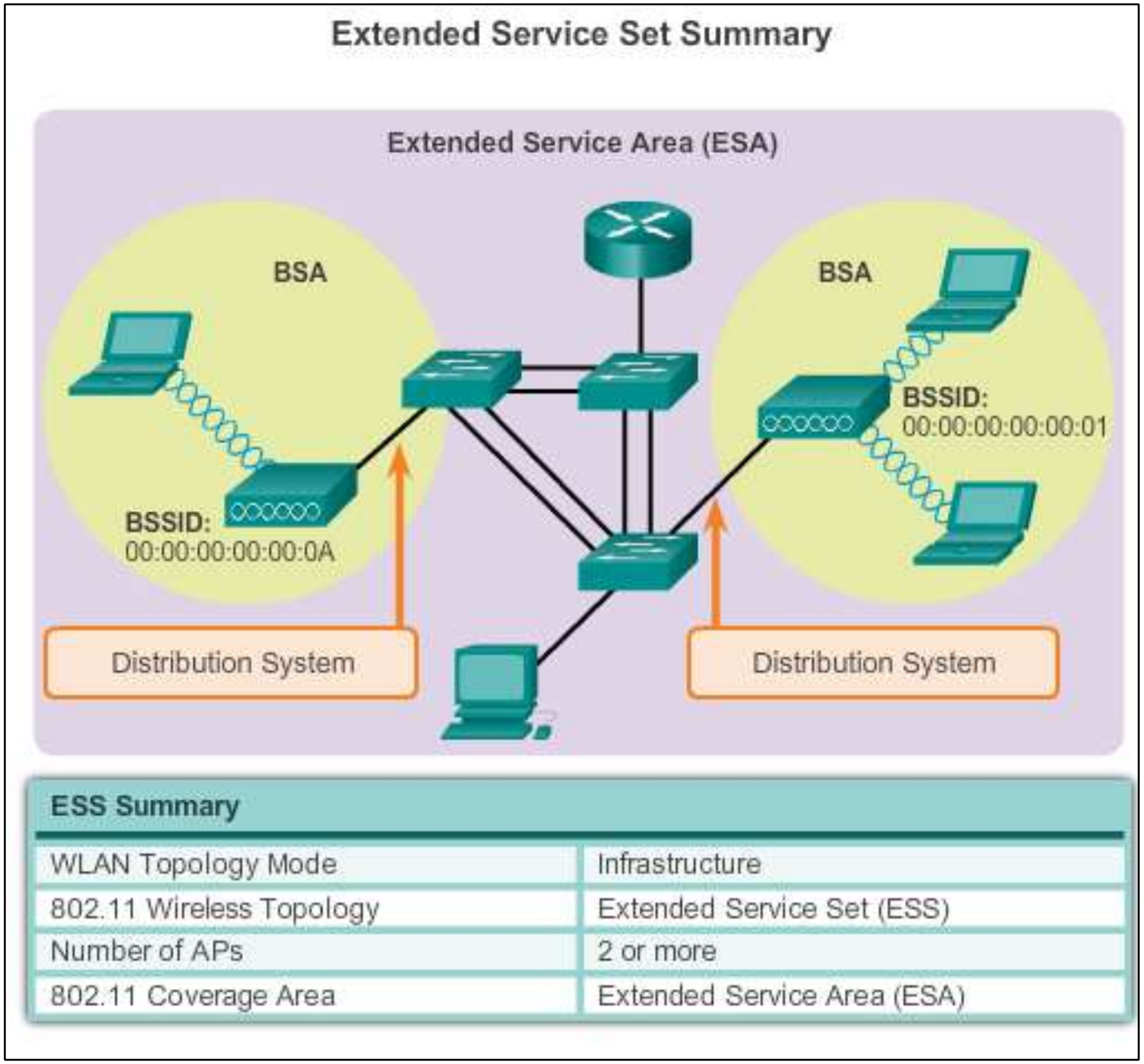


Basic Service Set Summary

BSS Summary	
WLAN Topology Mode	Infrastructure
802.11 Wireless Topology	Basic Service Set (BSS)
Number of APs	1
802.11 Coverage Area	Basic Service Area (BSA)

802.11 WLAN Topologies

Infrastructure Mode (cont.)



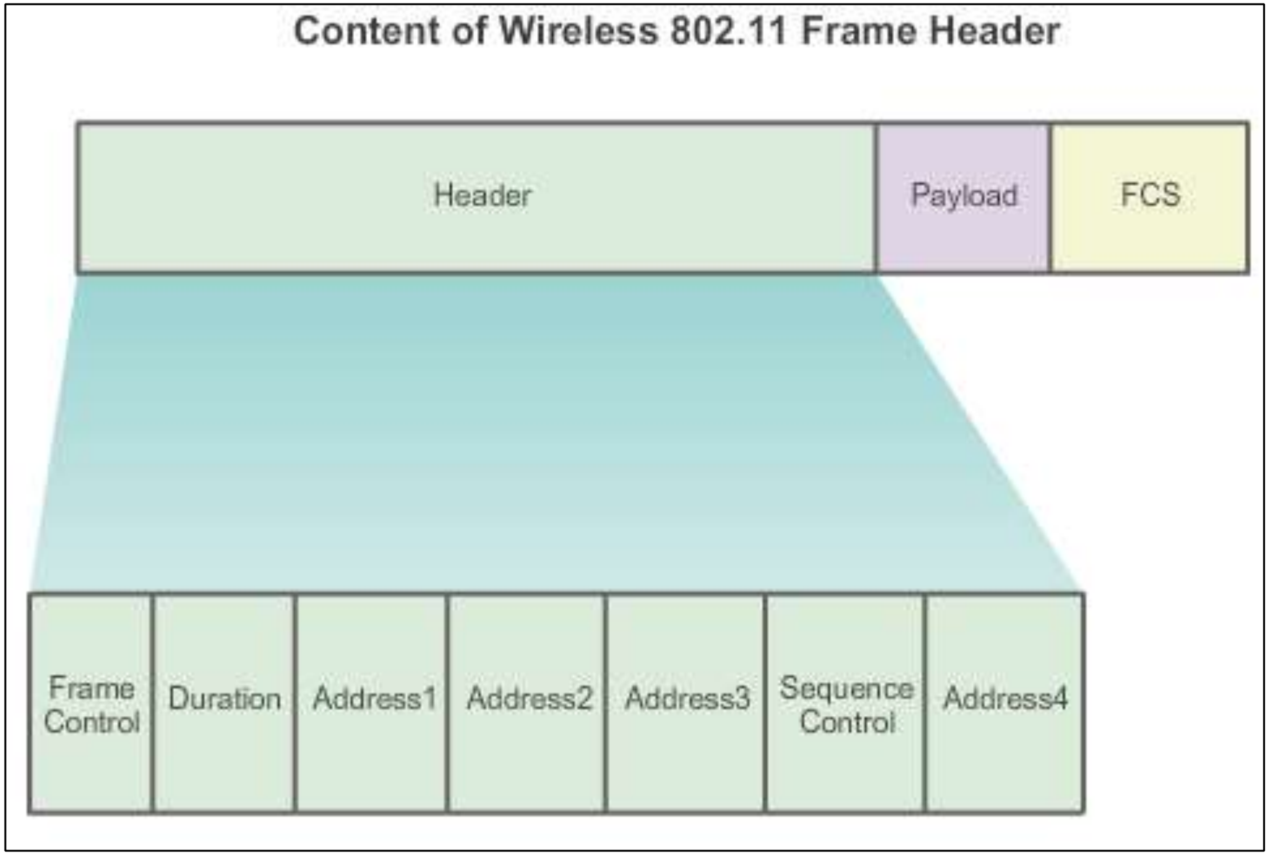
Extended Service Set Summary

ESS Summary	
WLAN Topology Mode	Infrastructure
802.11 Wireless Topology	Extended Service Set (ESS)
Number of APs	2 or more
802.11 Coverage Area	Extended Service Area (ESA)

4.2 Wireless LAN Operations

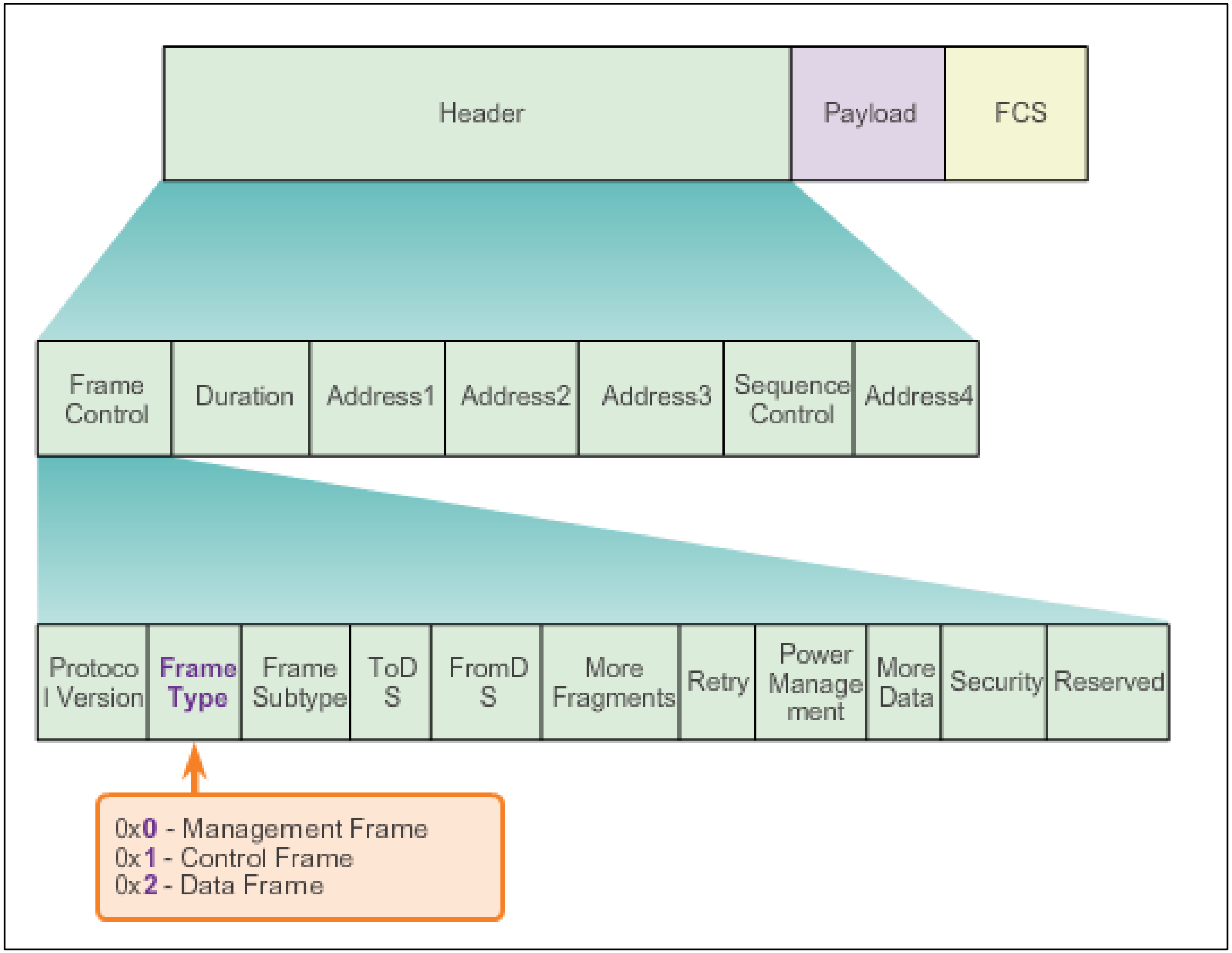
802.11 Frame Structure

Wireless 802.11 Frame



802.11 Frame Structure

Wireless Frame Type



Header	Payload	FCS

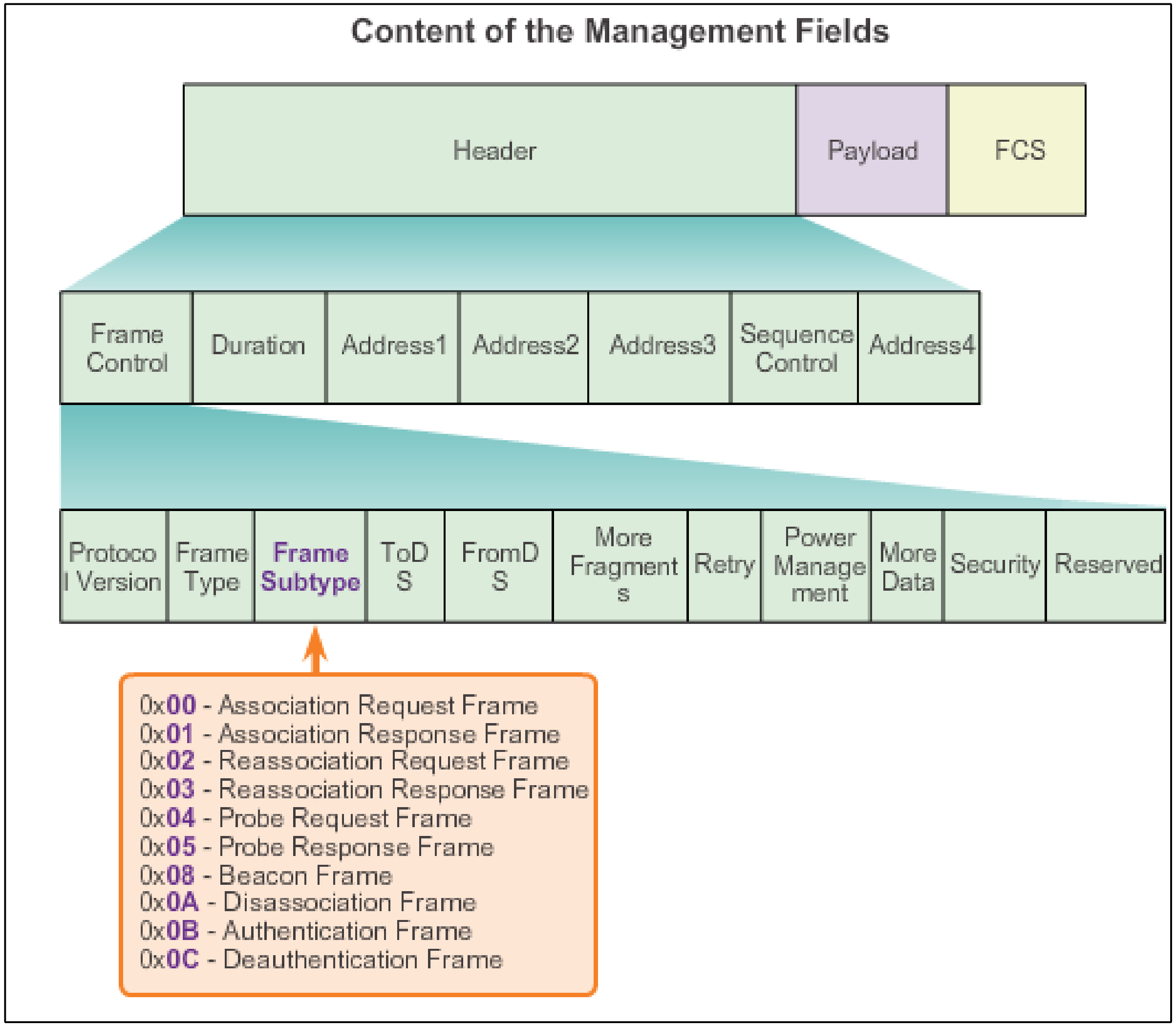
Frame Control	Duration	Address1	Address2	Address3	Sequence Control	Address4

Protocol Version	**Frame Type**	Frame Subtype	ToDS	FromDS	More Fragments	Retry	Power Management	More Data	Security	Reserved

0x**0** - Management Frame
0x**1** - Control Frame
0x**2** - Data Frame

802.11 Frame Structure

Management Frames



Content of the Management Fields

Header	Payload	FCS

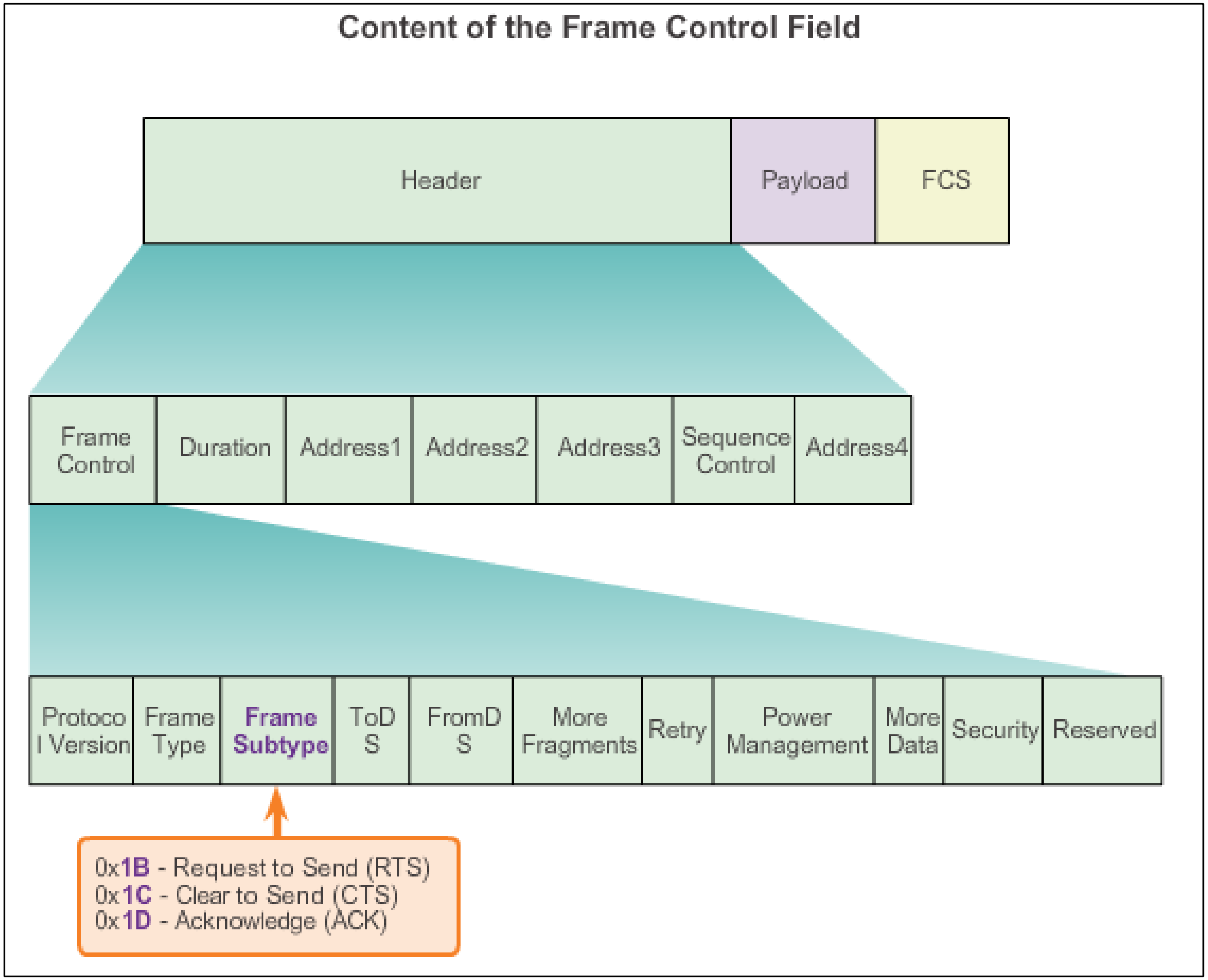
Frame Control	Duration	Address1	Address2	Address3	Sequence Control	Address4

Protocol Version	Frame Type	**Frame Subtype**	ToDS	FromDS	More Fragments	Retry	Power Management	More Data	Security	Reserved

0x**00** - Association Request Frame
0x**01** - Association Response Frame
0x**02** - Reassociation Request Frame
0x**03** - Reassociation Response Frame
0x**04** - Probe Request Frame
0x**05** - Probe Response Frame
0x**08** - Beacon Frame
0x**0A** - Disassociation Frame
0x**0B** - Authentication Frame
0x**0C** - Deauthentication Frame

802.11 Frame Structure

Control Frames

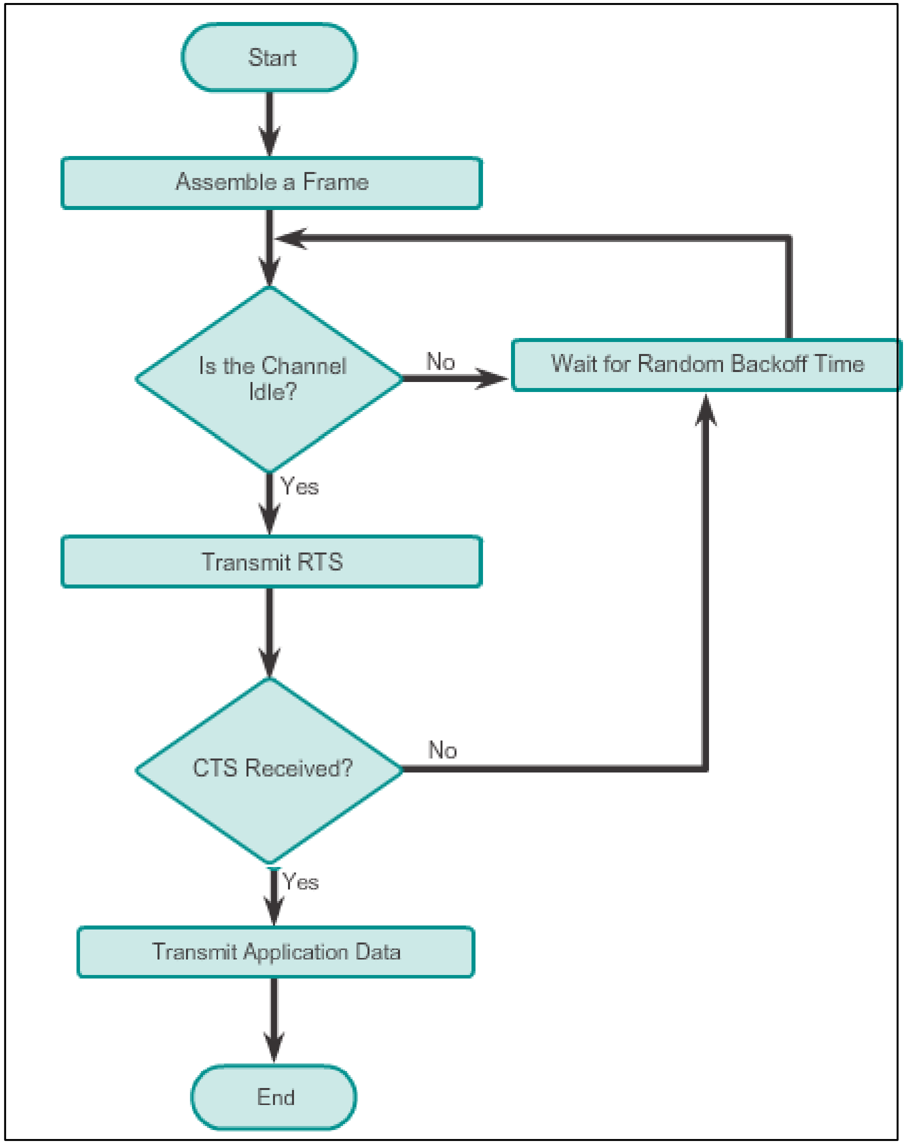


0x1B - Request to Send (RTS)
0x1C - Clear to Send (CTS)
0x1D - Acknowledge (ACK)

Wireless Operation

CSMA/CA

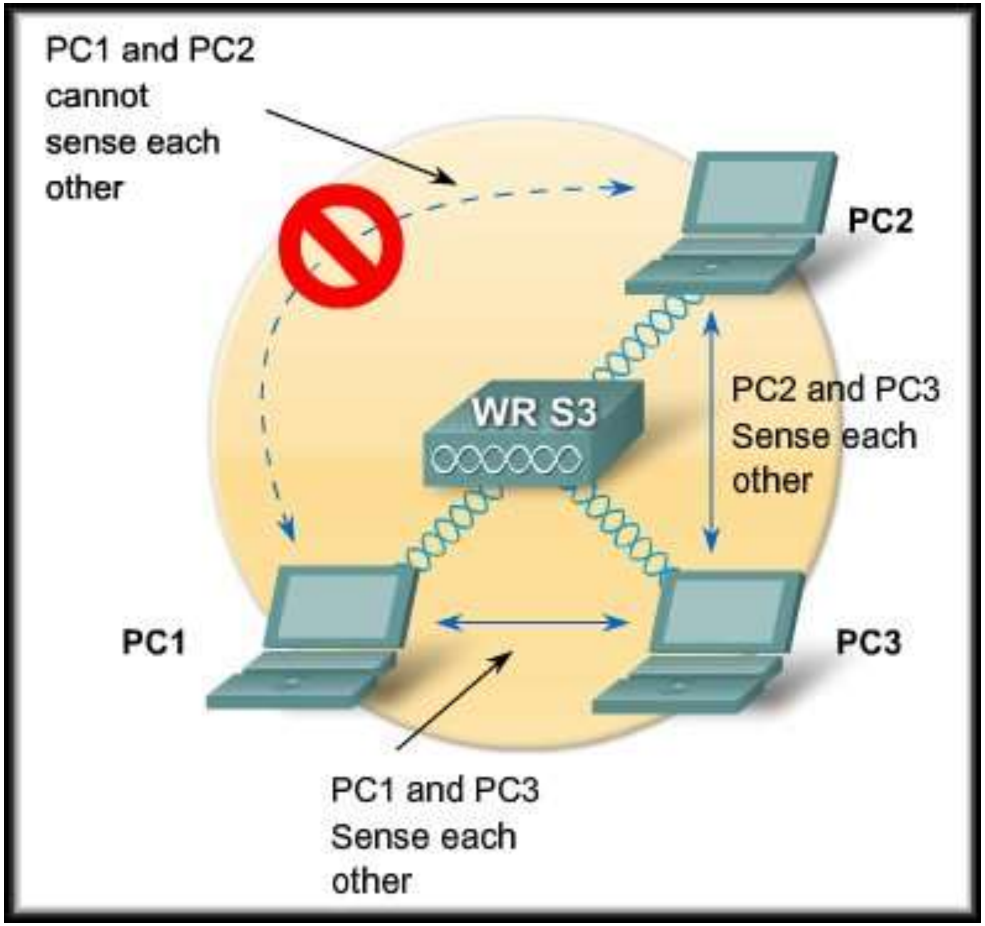
CSMA/CA Flowchart



Wireless Operation
CSMA/CA

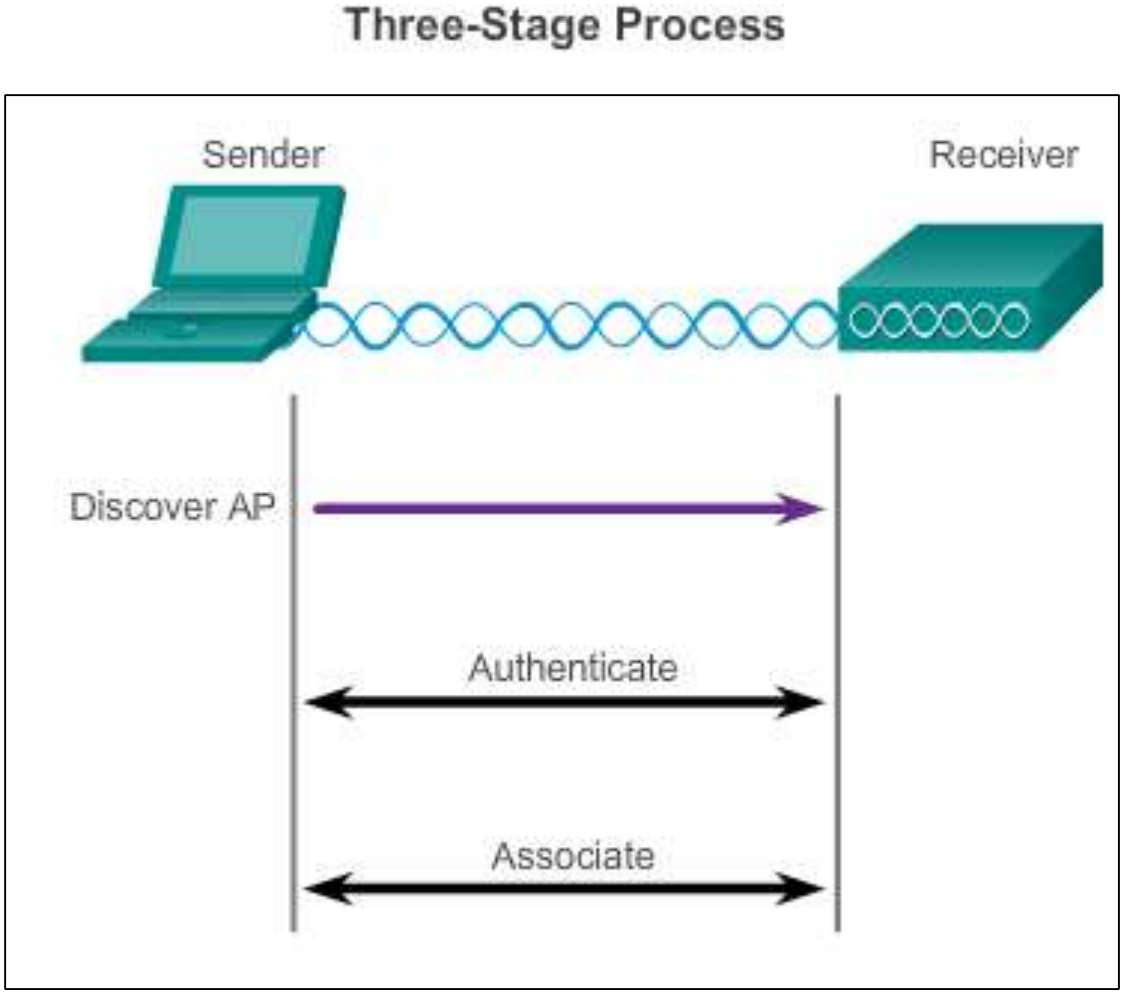
Why use CSMA/CA?

Hidden Node problem


PC1 and PC2 cannot sense each other
PC2
WR S3
PC2 and PC3 Sense each other
PC1
PC3
PC1 and PC3 Sense each other

Wireless Operation

Wireless Clients and Access Point Association



Wireless Operation

Association Parameters

- **SSID** – Unique identifier that wireless clients use to distinguish between multiple wireless networks in the same vicinity.
- **Password** – Required from the wireless client to authenticate to the AP. Sometimes called the security key.
- **Network mode** – Refers to the 802.11a/b/g/n/ac/ad WLAN standards. APs and wireless routers can operate in a mixed mode; i.e., it can simultaneously use multiple standards.
- **Security mode** – Refers to the security parameter settings, such as WEP, WPA, or WPA2.
- **Channel settings** – Refers to the frequency bands used to transmit wireless data. Wireless routers and AP can choose the channel setting or it can be manually set.

Wireless Operation

Discovering APs

Passive mode

- AP advertises its service by sending broadcast beacon frames containing the SSID, supported standards, and security settings.
- The beacon’s primary purpose is to allow wireless clients to learn which networks and APs are available in a given area.

Active mode

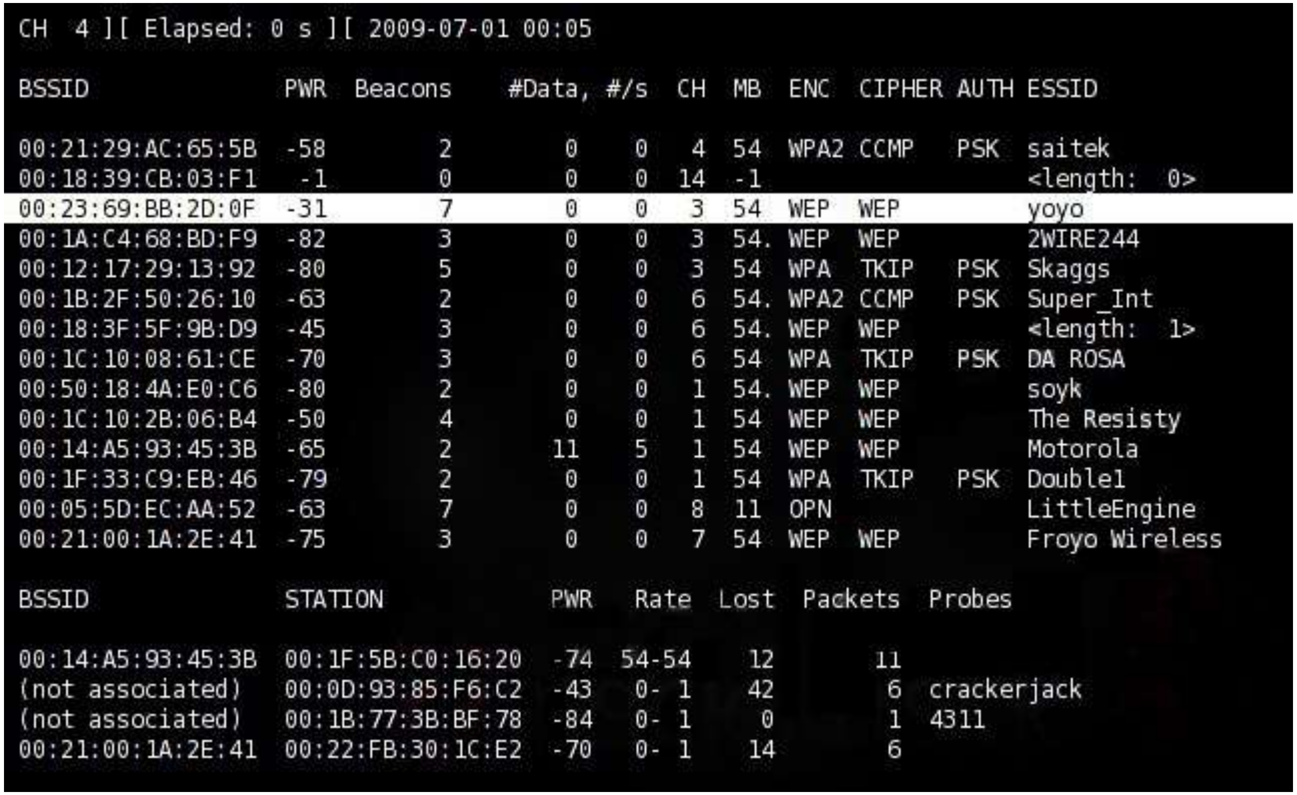
- Wireless clients must know the name of the SSID.
- Wireless client initiates the process by broadcasting a probe request frame on multiple channels.
- Probe request includes the SSID name and standards supported.
- May be required if an AP or wireless router is configured to not broadcast beacon frames.

Wireless Operation

Discovering APs

Active mode

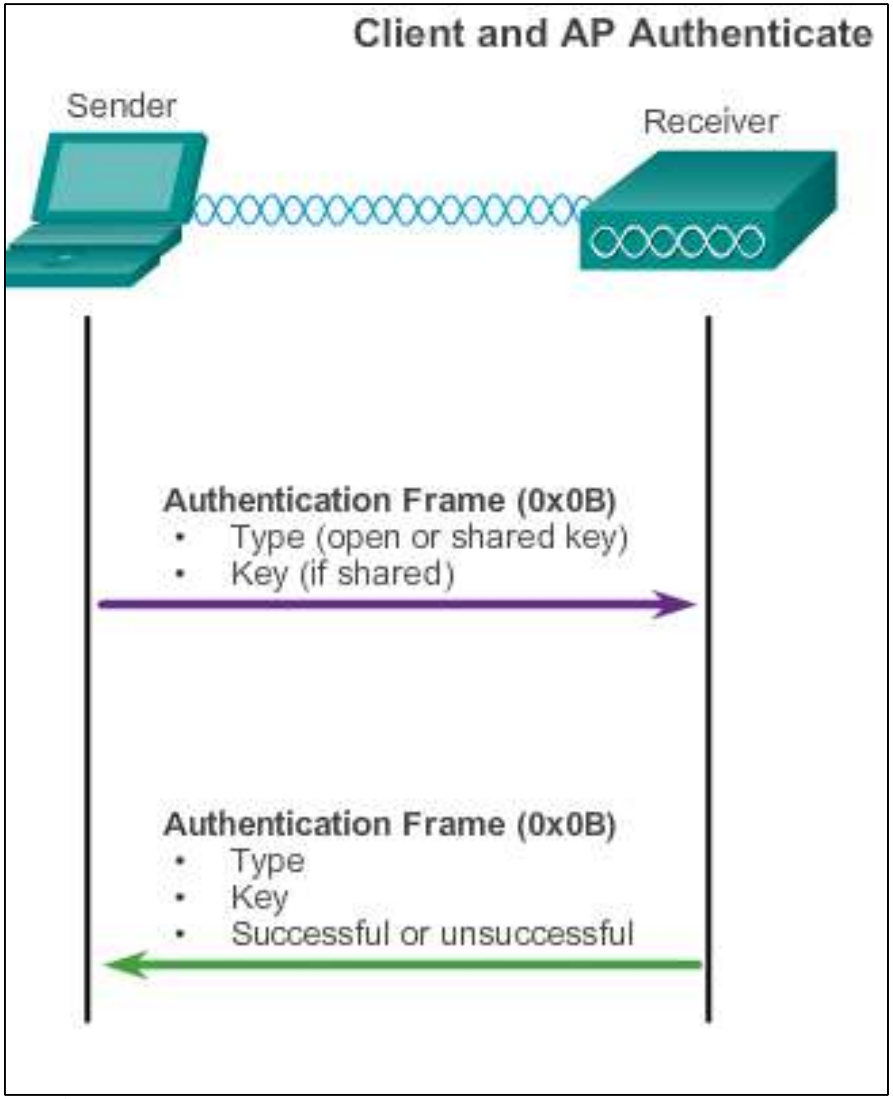
- Wireless clients always ask for the AP in there know network list



```
CH  4 ][ Elapsed: 0 s ][ 2009-07-01 00:05

BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:21:29:AC:65:5B  -58        2        0    0   4  54  WPA2 CCMP   PSK  saitek
00:18:39:CB:03:F1   -1        0        0    0  14  -1                   <length:  0>
00:23:69:BB:2D:0F  -31        7        0    0   3  54  WEP  WEP         yoyo
00:1A:C4:68:BD:F9  -82        3        0    0   3  54. WEP  WEP         2WIRE244
00:12:17:29:13:92  -80        5        0    0   3  54  WPA  TKIP   PSK  Skaggs
00:1B:2F:50:26:10  -63        2        0    0   6  54. WPA2 CCMP   PSK  Super_Int
00:18:3F:5F:9B:D9  -45        3        0    0   6  54. WEP  WEP         <length:  1>
00:1C:10:08:61:CE  -70        3        0    0   6  54  WPA  TKIP   PSK  DA ROSA
00:50:18:4A:E0:C6  -80        2        0    0   1  54. WEP  WEP         soyk
00:1C:10:2B:06:B4  -50        4        0    0   1  54  WEP  WEP         The Resisty
00:14:A5:93:45:3B  -65        2       11    5   1  54  WEP  WEP         Motorola
00:1F:33:C9:EB:46  -79        2        0    0   1  54  WPA  TKIP   PSK  Double1
00:05:5D:EC:AA:52  -63        7        0    0   8  11  OPN              LittleEngine
00:21:00:1A:2E:41  -75        3        0    0   7  54  WEP  WEP         Froyo Wireless

BSSID              STATION            PWR   Rate   Lost  Packets  Probes

00:14:A5:93:45:3B  00:1F:5B:C0:16:20  -74  54-54    12       11
(not associated)   00:0D:93:85:F6:C2  -43   0- 1    42        6  crackerjack
(not associated)   00:1B:77:3B:BF:78  -84   0- 1     0        1  4311
00:21:00:1A:2E:41  00:22:FB:30:1C:E2  -70   0- 1    14        6
```

Wireless Operation

Authentication


Client and AP Authenticate
Sender
Receiver
Authentication Frame (0x0B)
• Type (open or shared key)
• Key (if shared)
Authentication Frame (0x0B)
• Type
• Key
• Successful or unsuccessful

- **Open authentication** – A NULL authentication where the wireless client says “authenticate me” and the AP responds with “yes.” Used where security is of no concern.
- **Shared key authentication** – Technique is based on a key that is pre-shared between the client and the AP.

Channel Management

Frequency Channel Saturation

Direct-sequence spread spectrum (DSSS)

- Uses spread-spectrum modulation technique; designed to spread a signal over a larger frequency band making it more resistant to interference.
- Used by 802.11b.

Frequency-hopping spread spectrum (FHSS)

- Relies on spread-spectrum methods to communicate.
- Transmits radio signals by rapidly switching a carrier signal among many frequency channels.
- This channel-hopping process allows for a more efficient usage of the channels, decreasing channel congestion.
- Used by the original 802.11 standard.

Channel Management

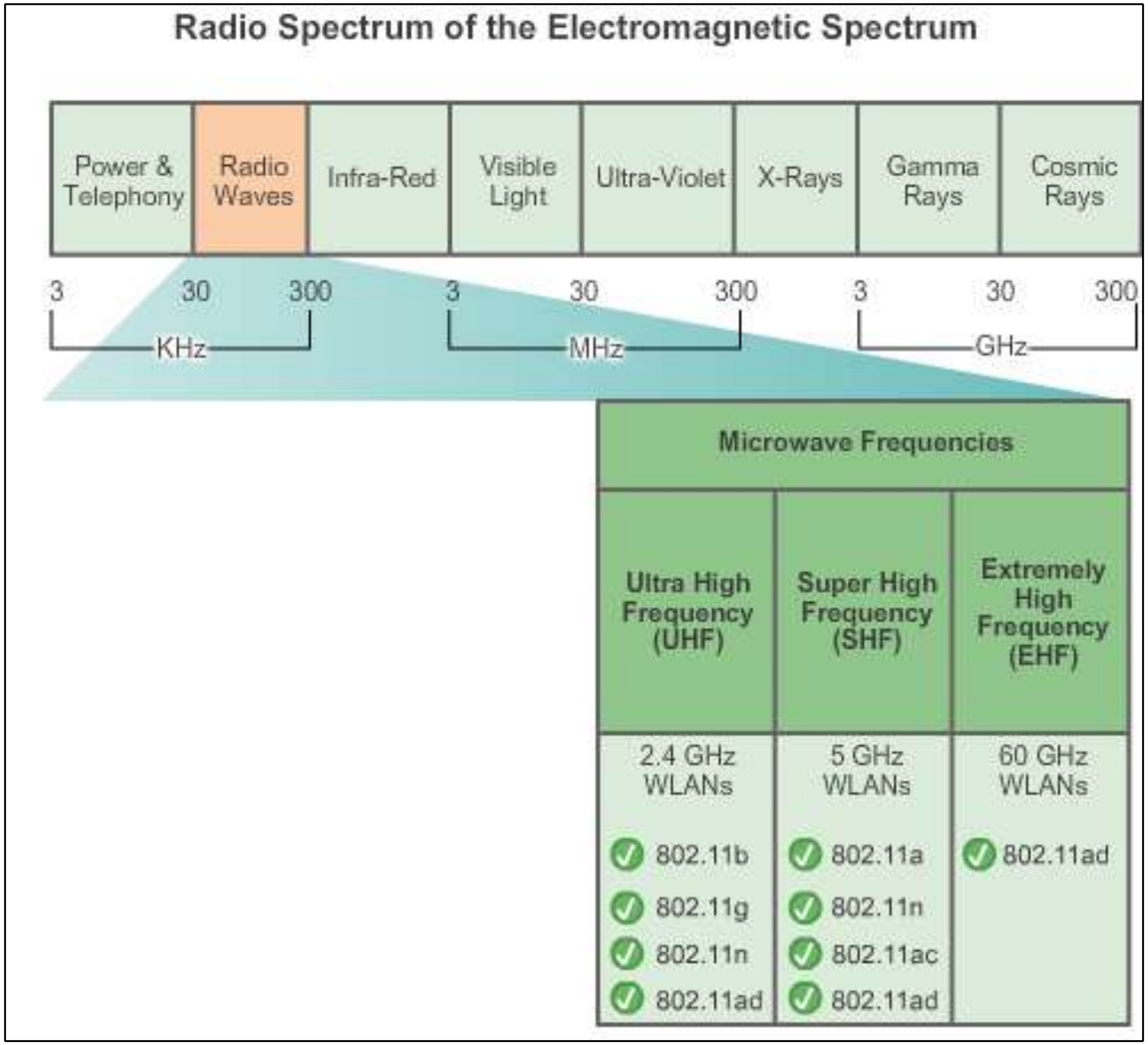
Frequency Channel Saturation (cont.)

Orthogonal Frequency-Division Multiplexing (OFDM)

- Subset of frequency division multiplexing in which a single channel utilizes multiple subchannels on adjacent frequencies.
- Because OFDM uses subchannels, channel usage is very efficient.
- Used by a number of communication systems, including 802.11a/g/n/ac.

Channel Management

Selecting Channels



Radio Spectrum of the Electromagnetic Spectrum

Power & Telephony | Radio Waves | Infra-Red | Visible Light | Ultra-Violet | X-Rays | Gamma Rays | Cosmic Rays

3 30 300 KHz

3 30 300 MHz

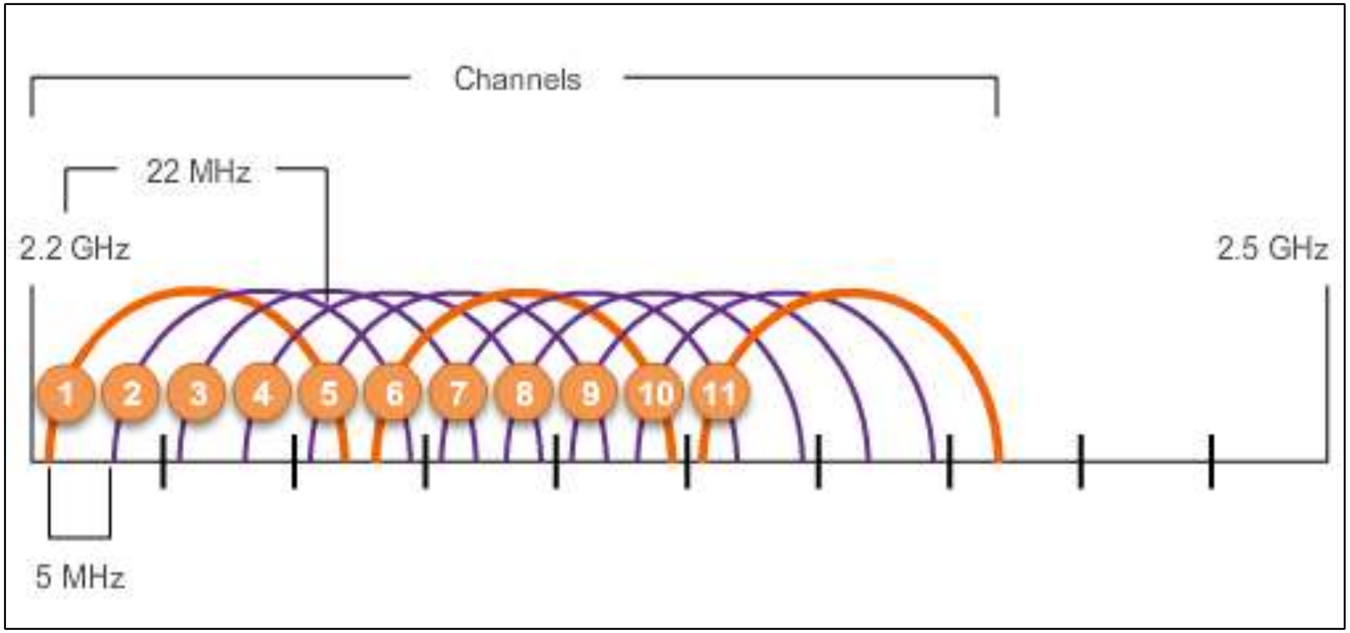
3 30 300 GHz

Microwave Frequencies		
Ultra High Frequency (UHF)	Super High Frequency (SHF)	Extremely High Frequency (EHF)
2.4 GHz WLANs	5 GHz WLANs	60 GHz WLANs
✓ 802.11b	✓ 802.11a	✓ 802.11ad
✓ 802.11g	✓ 802.11n	
✓ 802.11n	✓ 802.11ac	
✓ 802.11ad	✓ 802.11ad	

Channel Management

Selecting Channels (cont.)

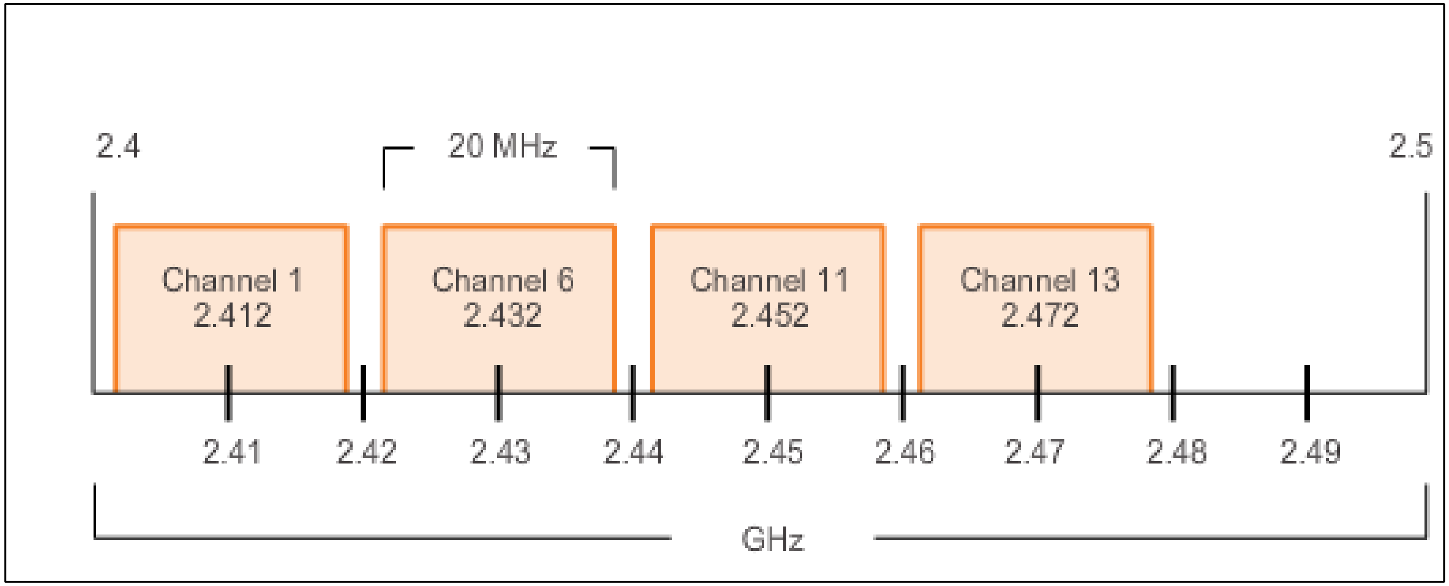
802.11b Channels



The solution to 802.11b interference is to use nonoverlapping channels 1, 6, and 11.

Selecting Channels (cont.)

802.11g/n (OFDM) Channel Width 20 MHz

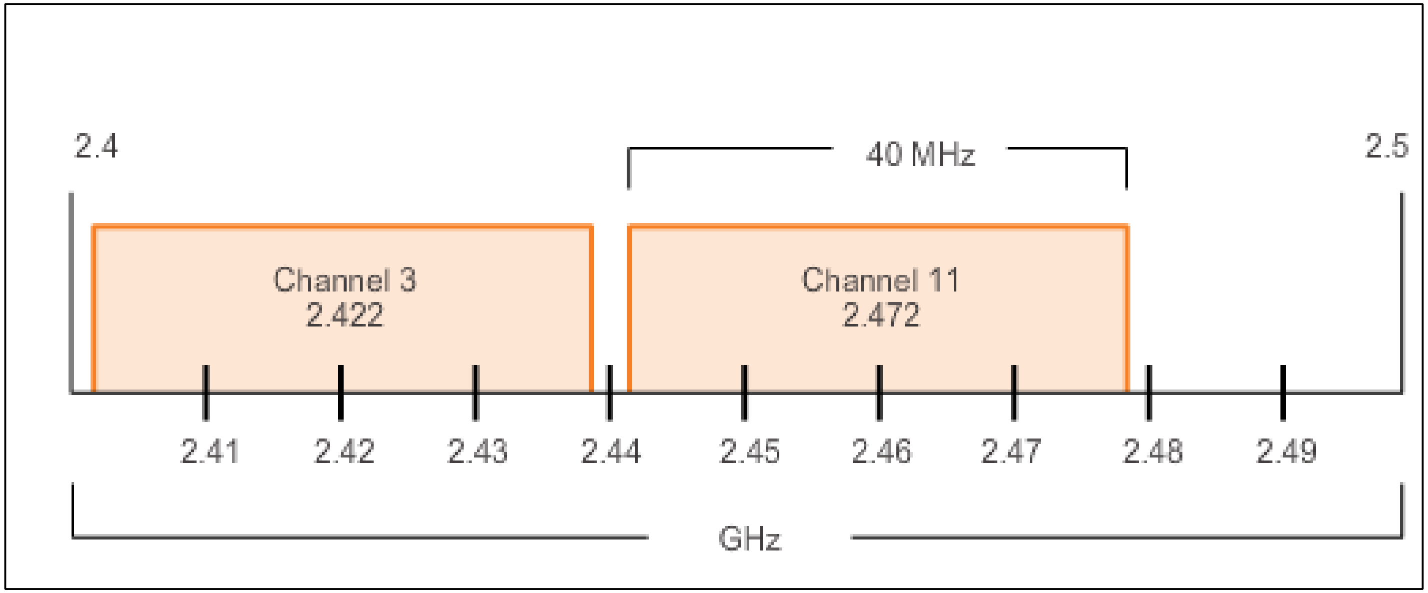


Use channels in the larger, less-crowded 5 GHz band, reducing “accidental denial of service (DoS),” this band can support four non-overlapping channels.

Channel Management

Selecting Channels (cont.)

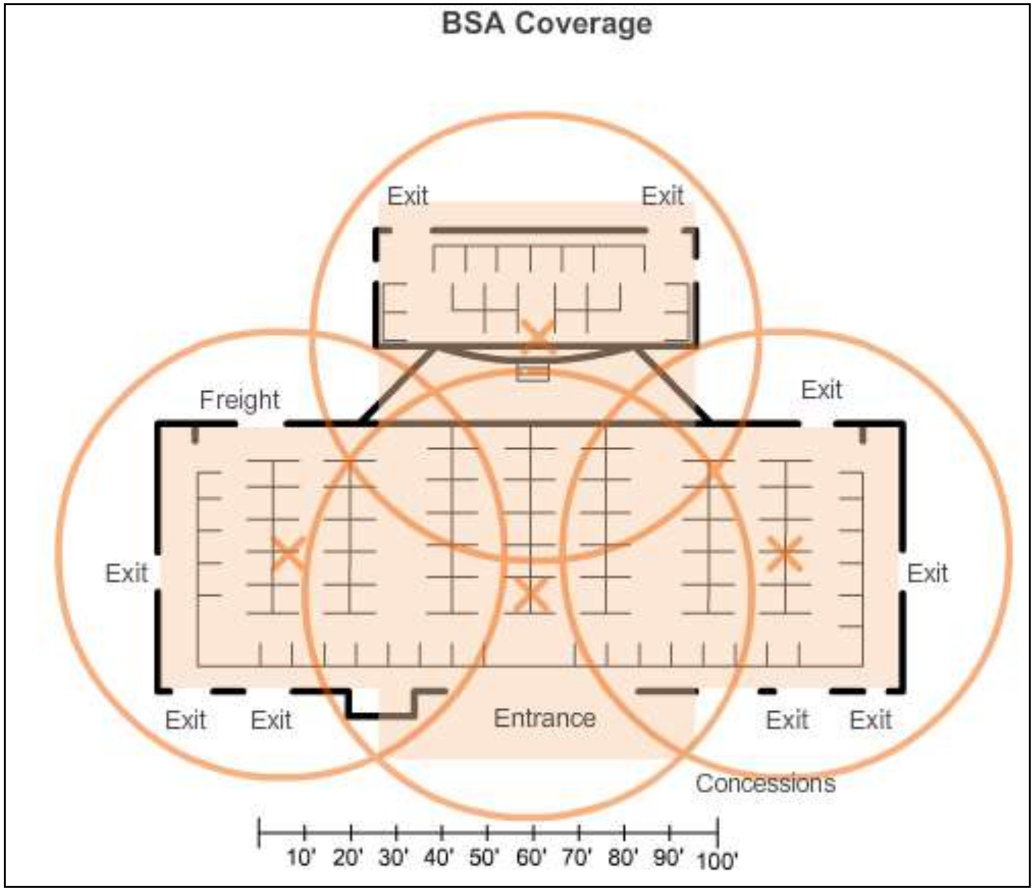
802.11n (OFDM) Channel Width 40 MHz



Channel bonding combines two 20-MHz channels into one 40-MHz channel.

Channel Management

Planning a WLAN Deployment



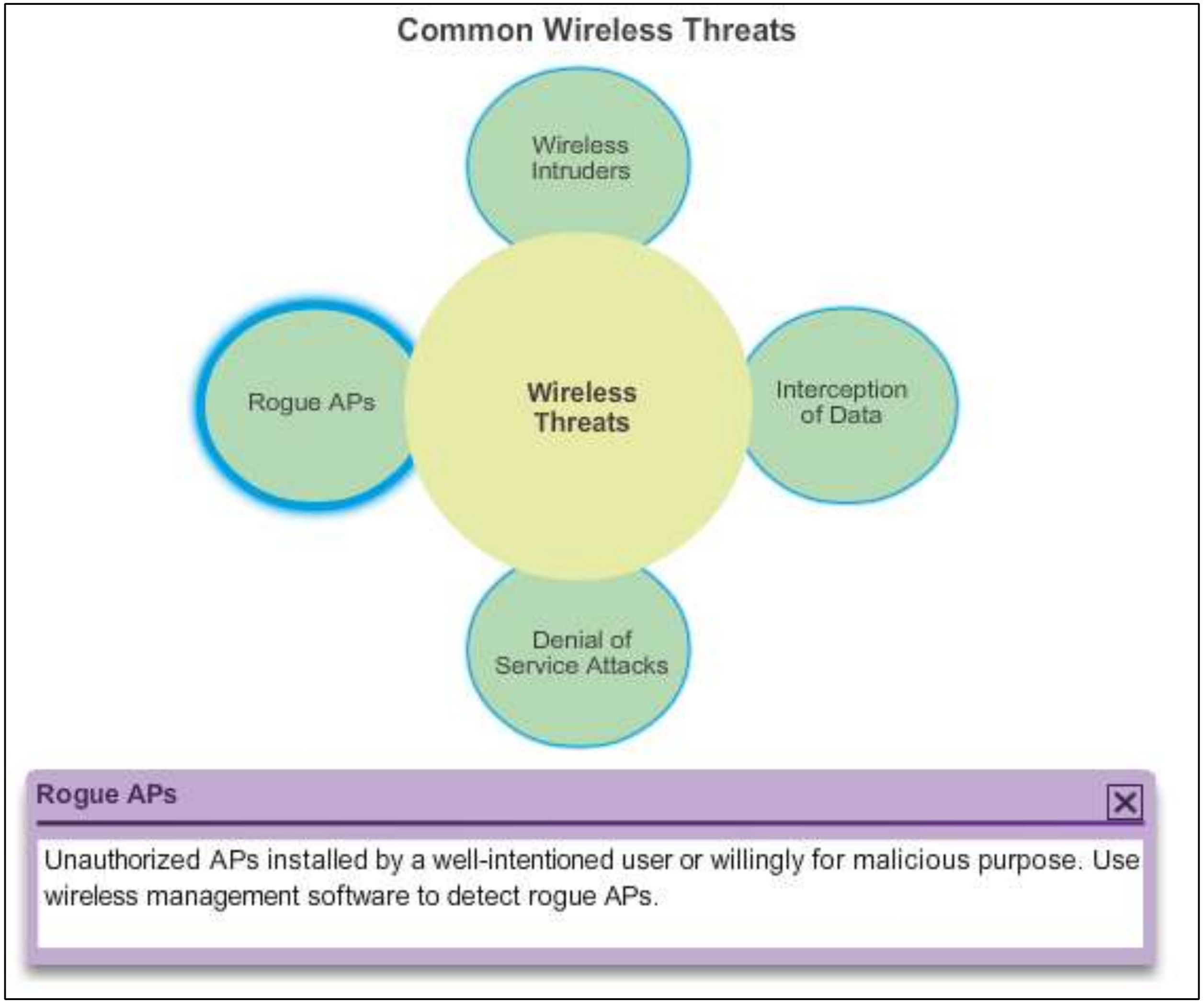
- If APs are to use existing wiring, or if there are locations where APs cannot be placed, note these locations on the map.
- Position APs above obstructions.
- Position APs vertically near the ceiling in the center of each coverage area, if possible.
- Position APs in locations where users are expected to be.

4.3 Wireless LAN Security

Cisco | Networking Academy®
Mind Wide Open™

WLAN Threats

Securing Wireless



Rogue APs

Unauthorized APs installed by a well-intentioned user or willingly for malicious purpose. Use wireless management software to detect rogue APs.

WLAN Threats

DoS Attack

Wireless DoS attacks can be the result of:

- Improperly configured devices.
- Configuration errors can disable the WLAN.
- A malicious user intentionally interfering with the wireless communication. Disable the wireless network where no legitimate device can access the medium.

Accidental interference

- WLANs operate in the unlicensed frequency bands and are prone to interference from other wireless devices.
- May occur from such devices as microwave ovens, cordless phones, baby monitors, and more.
- 2.4 GHz band is more prone to interference than the 5 GHz band.

WLAN Threats

Management Frame DoS Attacks

A spoofed disconnect attack

- Occurs when an attacker sends a series of “disassociate” commands to all wireless clients.
- Cause all clients to disconnect.
- The wireless clients immediately try to re-associate, which creates a burst of traffic.

A CTS flood

- An attacker takes advantage of the CSMA/CA contention method to monopolize the bandwidth.
- The attacker repeatedly floods Clear to Send (CTS) frames to a bogus STA.
- All wireless clients sharing the RF medium receive the CTS and withhold transmissions until the attacker stops transmitting the CTS frames.

WLAN Threats

Rogue Access Points

A rogue AP is an AP or wireless router that has been:

- Connected to a corporate network without explicit authorization and against corporate policy.
- Connected or enabled by an attacker to capture client data, such as the MAC addresses of clients (both wireless and wired), or to capture and disguise data packets, to gain access to network resources, or to launch man-in-the-middle (MITM) attacks.
- To prevent the installation of rogue APs, organizations must use monitoring software to actively monitor the radio spectrum for unauthorized APs.

WLAN Threats

Man-in-the-Middle Attack

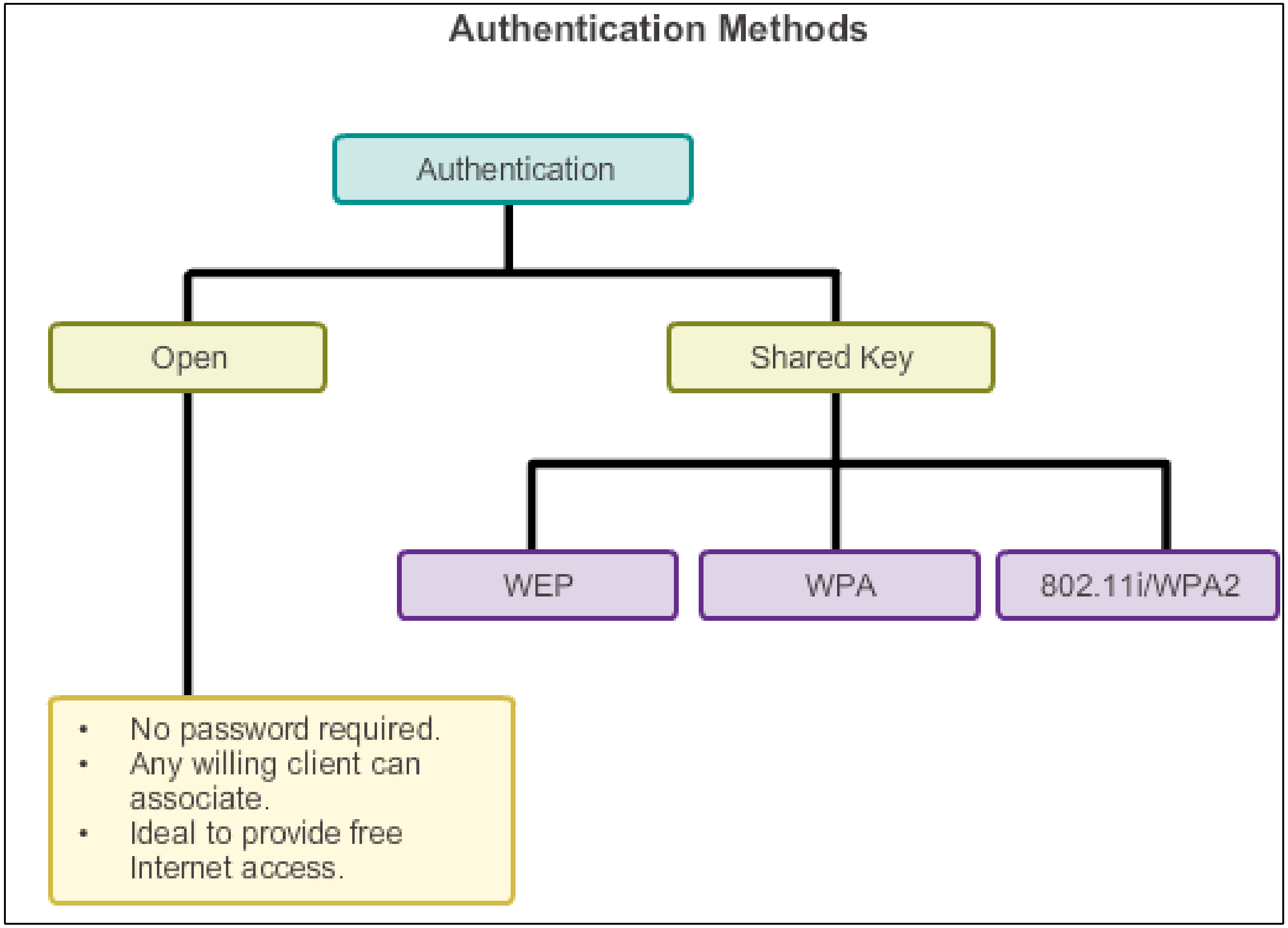
“Evil twin AP” attack:

- A popular wireless MITM attack where an attacker introduces a rogue AP and configures it with the same SSID as a legitimate AP.
- Locations offering free Wi-Fi, such as airports, cafes, and restaurants, are hotbeds for this type of attack due to the open authentication.
- Connecting wireless clients would see two APs offering wireless access. Those near the rogue AP find the stronger signal and most likely associate with the evil twin AP. User traffic is now sent to the rogue AP, which in turn captures the data and forwards it to the legitimate AP.
- Return traffic from the legitimate AP is sent to the rogue AP, captured, and then forwarded to the unsuspecting STA.

Securing WLANs

Wireless Security Overview

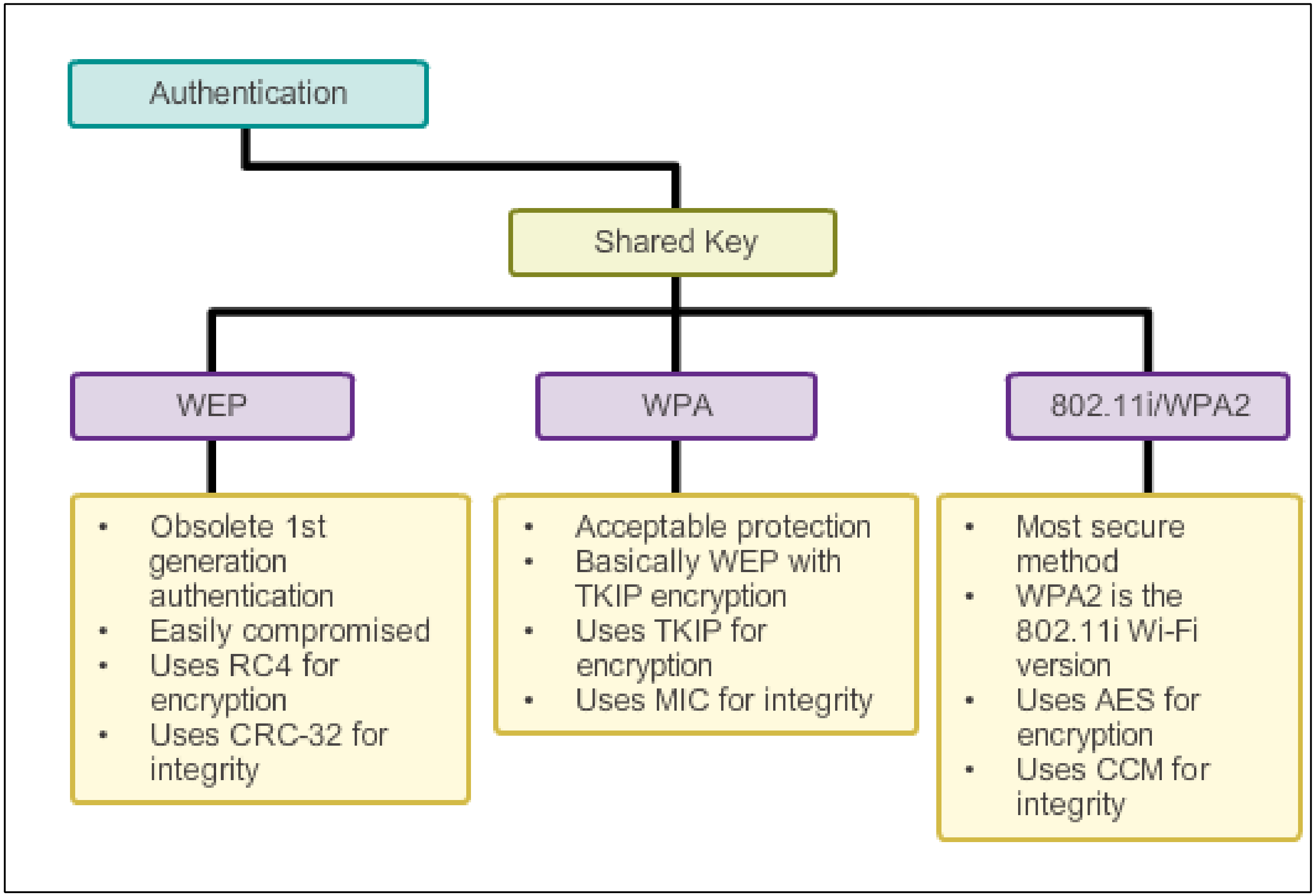
Use authentication and encryption to secure a wireless network.



- No password required.
- Any willing client can associate.
- Ideal to provide free Internet access.

Securing WLANs

Shared Key Authentication Methods



WEP:

- Obsolete 1st generation authentication
- Easily compromised
- Uses RC4 for encryption
- Uses CRC-32 for integrity

WPA:

- Acceptable protection
- Basically WEP with TKIP encryption
- Uses TKIP for encryption
- Uses MIC for integrity

802.11i/WPA2:

- Most secure method
- WPA2 is the 802.11i Wi-Fi version
- Uses AES for encryption
- Uses CCM for integrity

Securing WLANs

Encryption Methods

IEEE 802.11i and the Wi-Fi Alliance WPA and WPA2 standards use the following encryption protocols:

- **Temporal Key Integrity Protocol (TKIP)**
  - Used by WPA.
  - Makes use of WEP, but encrypts the Layer 2 payload using TKIP, and carries out a Cisco Message Integrity Check (MIC).
- **Advanced Encryption Standard (AES)**
  - Encryption method used by WPA2.
  - Preferred method because it aligns with the industry standard IEEE 802.11iA.
  - Stronger method of encryption.
  - Uses the Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP).
  - Always choose WPA2 with AES when possible.

Authenticating a Home User

WPA and WPA2 support two types of authentication:

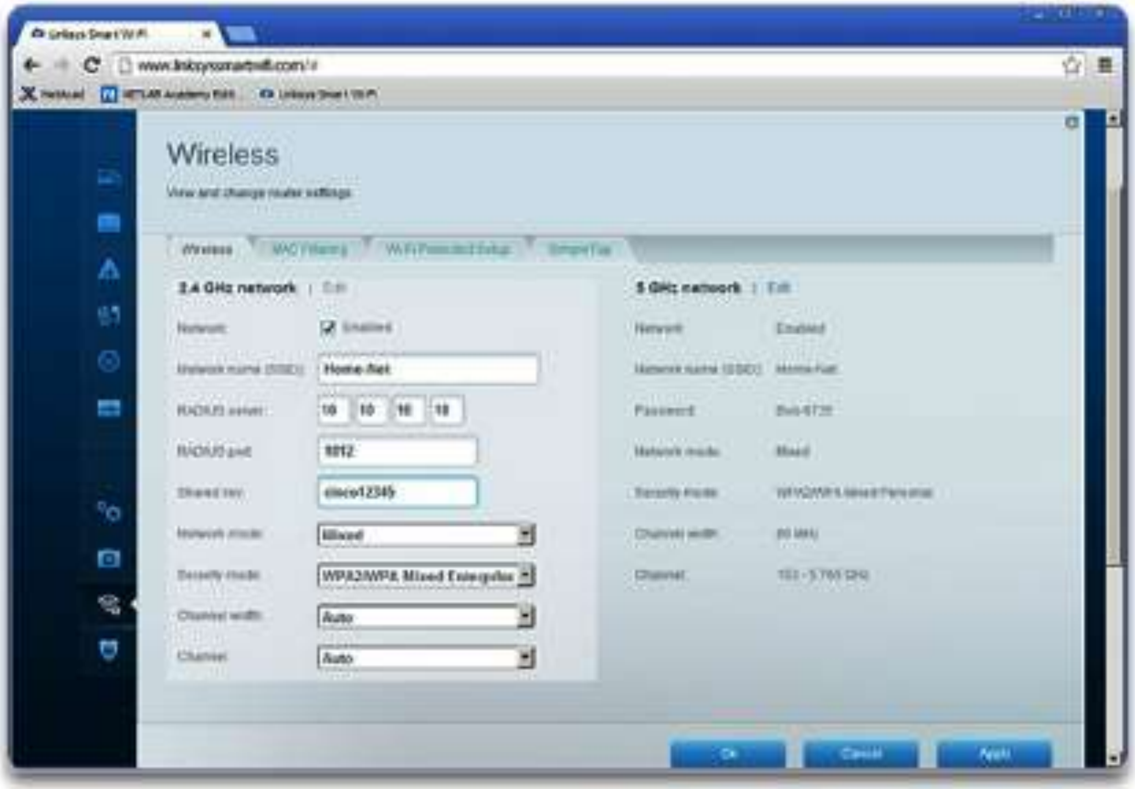
- **Personal**
  - Intended for home or small office networks, or authenticated users who use a pre-shared key (PSK).
  - No special authentication server is required.
- **Enterprise**
  - Requires a Remote Authentication Dial-In User Service (RADIUS) authentication server.
  - Provides additional security.
  - Users must authenticate using 802.1X standard, which uses the Extensible Authentication Protocol (EAP) for authentication.

Securing WLANs

Authentication in the Enterprise

Enterprise security mode choices require an Authentication, Authorization, and Accounting (AAA) RADIUS server.

Entering the RADIUS Server Specifics



2.4 GHz network | Edit

Network: ☑ Enabled
Network name (SSID): Home-Net
RADIUS server: 10 10 10 10
RADIUS port: 1812
Shared key: cisco12345
Network mode: Mixed
Security mode: WPA2/WPA Mixed Enterprise
Channel width: Auto
Channel: Auto

5 GHz network | Edit

Network: Enabled
Network name (SSID): Home-Net
Password: [illegible]
Network mode: Mixed
Security mode: WPA2/WPA Mixed Personal
Channel width: 80 MHz
Channel: 153 - 5.765 GHz

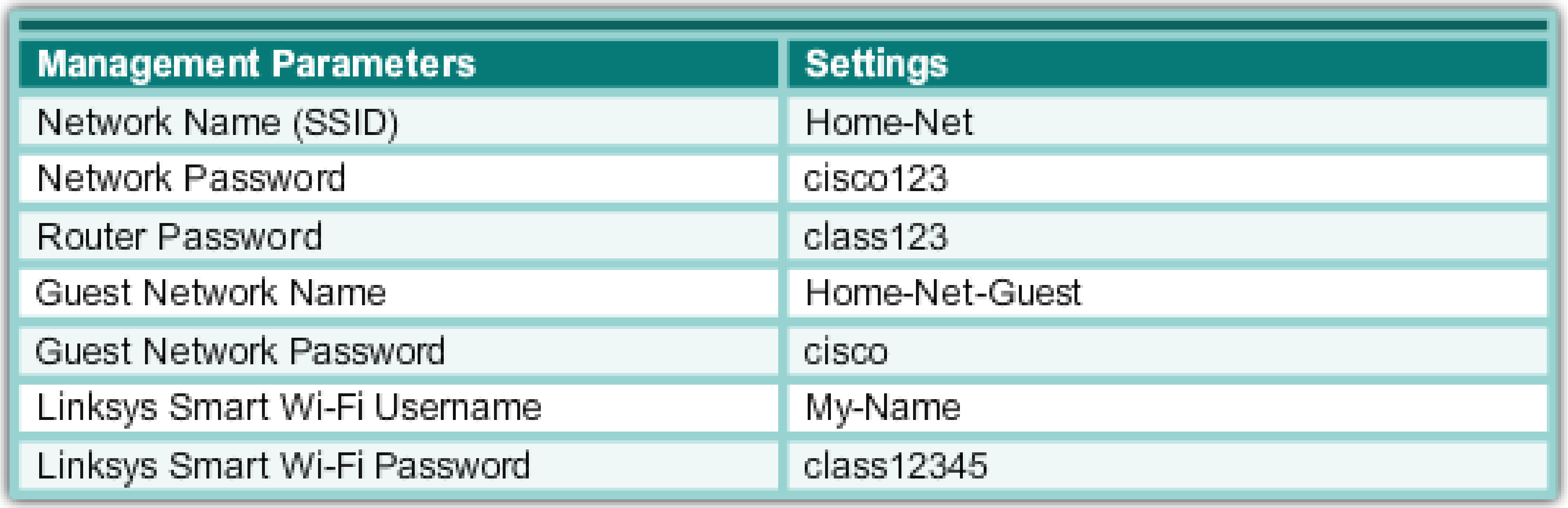
8.4 Wireless LAN Configuration

Cisco | Networking Academy®
Mind Wide Open™

Configure a Wireless Router

Configuring a Wireless Router

Before installing a wireless router, consider the following settings:



Management Parameters	Settings
Network Name (SSID)	Home-Net
Network Password	cisco123
Router Password	class123
Guest Network Name	Home-Net-Guest
Guest Network Password	cisco
Linksys Smart Wi-Fi Username	My-Name
Linksys Smart Wi-Fi Password	class12345

Configuring Wireless Clients

Connecting Wireless Clients

- After the AP or wireless router has been configured, the wireless NIC on the client must be altered to allow it to connect to the WLAN.
- The user should verify that the client has successfully connected to the correct wireless network, because there may be many WLANs available with which to connect.

Troubleshoot WLAN Issues

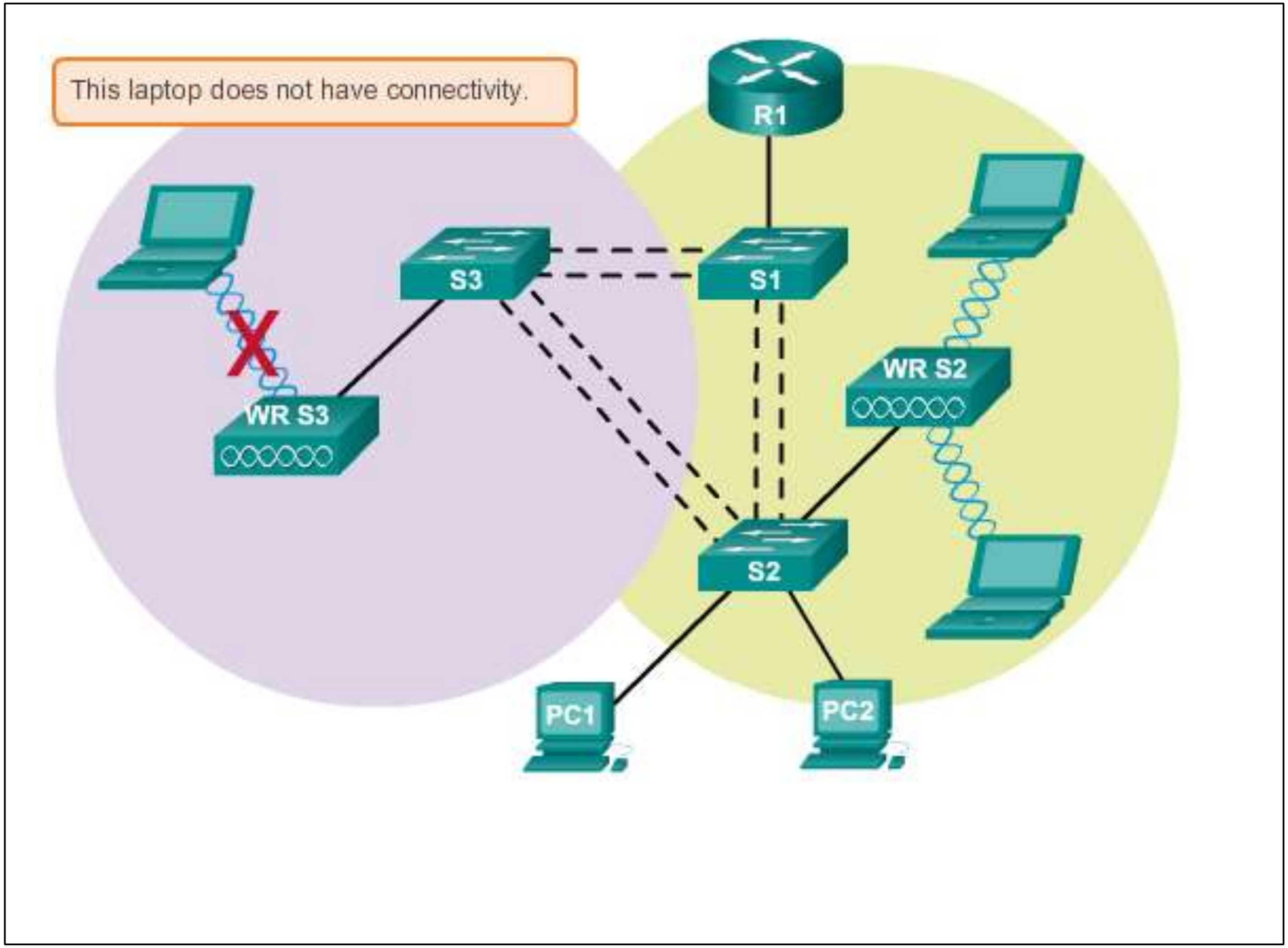
Troubleshooting Approaches

Three main troubleshooting approaches used to resolve network problems:

- **Bottom-up** – Start at Layer 1 and work up.
- **Top-down** – Start at the top layer and work down.
- **Divide-and-conquer** – Ping the destination. If the pings fail, verify the lower layers. If the pings are successful, verify the upper layers.

Troubleshoot WLAN Issues

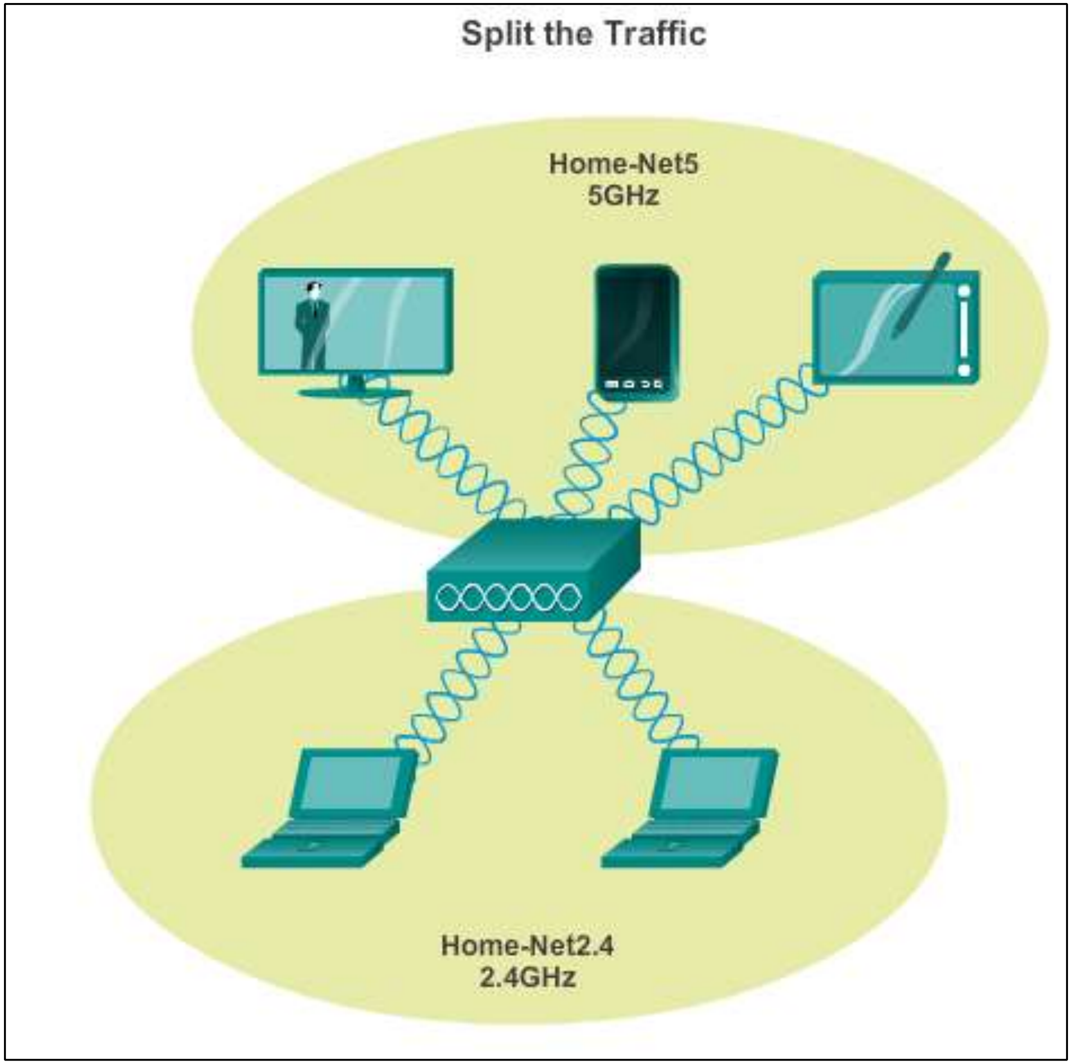
Wireless Client Not Connecting



This laptop does not have connectivity.

Troubleshoot WLAN Issues

Troubleshooting When the Network Is Slow



Cisco | Networking Academy®

Mind Wide Open™